Ruijie RG-CS86 Series Switches

CS86_RGOS 12.6(2)B0103

Command Reference

Document Version: V1.0
Date: 2023.04.27

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: https://www.ruijienetworks.com/rita

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in **bold** font.
Italic font	Arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Ruijie RG-CS86 Series Switches

CS86_RGOS 12.6(2)B0103

Command Reference

Document Version: V1.0
Date: 2023.04.27

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: https://www.ruijienetworks.com/rita

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in **bold** font.
Italic font	Arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Basic Configuration Commands

1 CLI Commands

Command	Function
alias	Configure an alias for a command.
cli-python	Load and unload the Python script of CLI.
language character-set	Configure the character set encoding format for the device.
privilege	Configure the privilege level of a command.
show aliases	Display all command aliases or the command aliases in specific command modes.

1.1 alias

Function

Run the **alias** command to configure an alias for a command.

Run the **no** form of this command to delete the custom alias of a command. Then, the default alias of a command that has a default alias can be restored.

Run the **default** form of this command to restore the default configuration for a command that has a default alias.

Default aliases are available for some commands in global configuration mode or privileged EXEC mode by default.

Syntax

alias *mode command-alias original-command*

no alias *mode* [*command-alias*]

default alias *mode* [*command-alias*]

Parameter Description

mode: Name of the configuration mode of the command represented by an alias in the system.

command-alias: Command alias.

original-command: Actual command syntax represented by the alias.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- In privileged EXEC mode, the actual commands whose default aliases are h, p, s, u, and un are **help**, **ping**, **show**, **undebug**, and **undebug** respectively.
- A default command alias cannot be deleted by using the **no alias exec** command.
- You can configure a command alias to replace a command with one word. For example, you can create an alias to represent the front part of a command, and then enter the part other than the alias of the command.
- The command represented by an alias is in a command mode that already exists in the current system. In global configuration mode, you can run the **alias ?** command to list all command modes that can be configured with aliases.

```
Hostname(config)# alias ?
aaa-gs              AAA server group mode
acl                 acl configure mode
bgp                 Configure bgp Protocol
config              globle configure mode
```

- The system provides help information for command aliases. An asterisk (*) is displayed in front of an alias

and the help information is displayed in the following format:

```
*command-alias=original-command
```

For example, in privileged EXEC mode, the default command alias "s" represents the keyword **show**. If you enter "s?", help information of the keywords and aliases starting with "s" is displayed.

```
Hostname# s?
*s=show  show  start-chat  start-terminal-service
```

- If the command represented by an alias contains more than one word, the command is displayed in a pair of quotation marks. For example, in privileged EXEC mode, configure the alias "sv" to replace the **show version** command.

```
Hostname# s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

- An alias must start with the first character of a command line and no space is allowed before the alias. As shown in the example above, if you enter a space in front of the command, the alias becomes an invalid alias.

```
Hostname# s?
show  start-chat  start-terminal-service
```

- The system also provides help information of command parameters for a command alias. For example, if you configure the command alias "ia" in interface configuration mode to represent **ip address**, and enter **ia ?** in the interface configuration mode, the following notification is displayed.

```
Hostname(config-if)# ia ?
A.B.C.D  IP address
dhcp     IP Address via DHCP
Hostname(config-if)# ip address
```

Information of the parameters following the **ip address** command is provided and the command alias is replaced with the actual command.

- An alias must be entered in full when it is used; otherwise, it cannot be identified.
- You can use the **show aliases** command to display alias configuration in the system.

Examples

The following example configures the command alias "def-route" to represent the route configuration command **ip route 0.0.0.0 0.0.0.0 192.168.1.1** in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
Hostname(config)# def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
Hostname(config)# end
Hostname# show aliases config
globle configure mode alias:
def-route          ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Notifications

A command alias cannot be longer than19 characters. Otherwise, the following notification is displayed.

```
% Overly long alias name truncated after 19 characters.
```

The actual command string represented by an alias cannot be longer than 255 characters. Otherwise, the following notification is displayed.

```
% Command alias string too long.
```

A maximum of 100 aliases are supported in a single command mode. Otherwise, the following notification is displayed.

```
% Can't add more than 100 command aliases in single mode.
```

If an alias fails to be added due to various reasons (for example, insufficient memory), the following notification is displayed.

```
% Adding command alias fail.
```

Common Errors

N/A

Platform Description

On the command line interface (CLI), configure one word as the alias of one command. Enter this word. If it can replace this command, the configured alias is valid.

Related Commands

- **show aliases**

1.2 cli-python

Function

Run the **cli-python** command to load and unload the Python script of CLI.

Syntax

cli-python { **insmod** | **rmmod** } *python-filename*

Parameter Description

insmod *python-filename*: Loads the Python script of CLI. *python-filename* indicates the full name of the Python script file.

rmmod *python-filename*: Unloads the Python script of CLI. *python-filename* indicates the full name of the Python script file.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to upload the Python script file to the root directory of flash disk of the device and /data under shell, and run the Python loading command to load the Python script.

Examples

The following example loads the **Hostname.Py** script.

```
Hostname> enable
Hostname# cli-python insmod Hostname.py
% Python script module "Hostname.py" insert success.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 language character-set

Function

Run the **language character-set** command to configure the character set encoding format for the device.

Hybrid formats are supported by default.

Syntax

language character-set { **default** | **GBK** | **UTF-8** }

Parameter Description

default: Sets the character set encoding format to the default format (hybrid formats supported).

GBK: Sets the character set encoding format to GBK.

UTF-8: Sets the character set encoding format to UTF-8.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When hybrid formats exist in current running configurations, you must manually delete running configurations containing the encoding format different from the target format before modifying the character set encoding format.

Examples

The following example sets the character set encoding format of the device to UTF-8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# language character-set UTF-8
This may take some time to build configuration, Continue? (yes[no]): y
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 privilege

Function

Run the **privilege** command to configure the privilege level of a command.

Run the **no** form of this command to restore the privilege level of the command to the default value.

Syntax

privilege *mode* [**all**] { **level** *level* | **reset** } *command-string*

no privilege *mode* [**all**] [**level** *level*] *command-string*

Parameter Description

mode: Name of the configuration mode of the command. Whether this parameter is supported depends on the actual product version.

all: Changes the privilege levels of all subcommands contained in a specific command to the same level.

level *level*: Specifies the privilege level of a command or a subcommand. The range is from 0 to 15.

reset: Restores the command privilege level to the default value.

command-string: Command string to be assigned with a privilege level.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- In global configuration mode, you can use the **privilege ?** command to display all CLI command modes, to which a privilege level is assigned. The number of command modes that can be assigned with a privilege level varies with products. Some command modes are described as follows:
  - config: Indicates the global configuration mode.
  - exec: Indicates the privileged EXEC mode.
  - interface: Indicates the interface configuration mode.
  - ip-dhcp-pool: Indicates the Dynamic Host Configuration Protocol (DHCP) address pool configuration mode.
  - keychain: Indicates the keychain configuration mode.
  - keychain-key: Indicates the keychain-key configuration mode.
  - time-range: Indicates the time-range configuration mode.
- Select a command which is supported for users at a higher privilege level (for example, privilege level 14) but is not supported for users at a lower privilege level (for example, privilege level 1), and then specify a lower privilege level for command execution. Switch the user to a lower privilege level. If this command can be executed, the permission is assigned.

Examples

The following example sets the password for users at privilege level 1 to access CLI to **test**, and sets the permission for running the **reload** command to reset the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# privilege exec level 1 reload
```

The following example verifies that users at privilege level 1 can access CLI to use the **reload** command.

```
Hostname> reload ?
LINE    Reason for reload
<cr>
```

The following example assigns the permission to run all subcommands of the **reload** command to users at privilege level 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# privilege exec all level 1 reload
```

The following example verifies that users at privilege level 1 can access CLI to use all subcommands of the **reload** command.

```
Hostname> reload ?
LINE    Reason for reload
at                  reload at a specific time/date
cancel              cancel pending reload scheme
```

```
in                  reload after a time interval
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show aliases

Function

Run the **show aliases** command to display all command aliases or the command aliases in specific command modes.

Syntax

show aliases [*mode*]

Parameter Description

mode: Command mode of the command represented by an alias.

Command Modes

All modes except user EXEC mode

Default Level

14

Usage Guidelines

If no command mode is entered, all command aliases you have set are displayed.

Examples

The following example displays the command aliases in privileged EXEC mode.

```
Hostname> enable
Hostname# show aliases exec
exec mode alias:
h                   help
p                   ping
s                   show
u                   undebug
un                  undebug
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 ZAM Commands

Command	Function
show zam	Display the current configurations and status of ZAM.
zam	Enable the ZAM function.

1.1 show zam

Function

Run the **show zam** command to display the current configurations and status of ZAM.

Syntax

show zam

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the current configurations and status of ZAM.

```
Hostname> enable
Hostname# show zam
ZAM state          : enable
ZAM status         : Now is idle
Server ip           :NULL
Usb path            :NULL
Interface name       :NULL
Interface type       :UNKNOWN
Succ Interface name   :NULL
Script URL          :NULL
```

Table 1-1 Output Fields of the show zam Command

Field	Description
ZAM state	Whether ZAM is enabled or disabled.
ZAM status	Current status of ZAM.
Server ip	IP address of the TFTP server.
Usb path	USB path.
Interface name	Interface name.
Interface type	Interface type.

Field	Description
Succ Interface name	Last fetched interface name.
Script URL	Script URL.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 zam

Function

Run the **zam** command to enable the ZAM function.

Run the **no** form of this command to disable the ZAM function.

The ZAM function is enabled by default.

Syntax

zam

no zam

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example disables the ZAM function.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# no zam
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show zam**

1 Basic Management Commands

Command	Function
banner	Configure a prompt.
boot config	Modify the storage path and name of the startup configuration file.
calendar set	Configure the hardware time of the system.
checkpoint	Configure a checkpoint.
clear checkpoint database	Clear checkpoints and related data.
clear telnet ip-block	Clear entries about blocked IP addresses and authentication failures.
clock read-calendar	Configure the system to synchronize the software time with the hardware time.
clock set	Configure the software time of the system.
clock summer-time	Configure the DST.
clock timezone	Configure a time zone.
clock update-calendar	Configure the system to synchronize the hardware time with the software time.
configure	Enter the global configuration mode.
cpu high-watermark set	Configure the maximum threshold for the total CPU usage of all control cores and enable CPU usage monitoring.
disconnect	Close a suspended telnet client session.
do telnet	Log in to the telnet server.
enable	Enter the privileged EXEC mode or switch a role.
enable default role	Configure the default role for running the enable commands.
enable password	Configure passwords for different privilege levels.
enable secret	Configure secure encrypted passwords for different privilege levels.
enable service	Enable a specified service.

end	Exit the current mode and return to the privileged EXEC mode.
exec-banner	Enable EXEC prompt information display for a specific line.
exec-timeout	Set the connection timeout time of the device on a line.
execute	Run commands in the batch file.
exit	Exit the configuration mode and return to the upper-level mode or exit the command line interface (CLI) from the privileged EXEC mode.
Help	Display a brief description of the help system.
hostname	Specify or modify the host name of the device.
ip telnet access-class	Configure an access control list (ACL) for the telnet server.
ip telnet ip-block	Configure the maximum number of consecutive authentication failures, beyond which an IP address is blocked on the telnet server, and to specify the period for awakening the blocked IP address.
ip telnet source-interface	Specify the IP address of an interface as the source IP address of a telnet connection.
ipv6 telnet access-class	Configure an IPv6 ACL for a telnet server.
lock	Set a temporary password on a terminal to lock the terminal CLI to prevent access while keeping the session.
lockable	Enable the locking feature for terminals connected to the current line.
login	Configure simple login password verification for a line.
login access non-aaa	Enable non-AAA authentication for a line when the AAA service is enabled.
login local	Configure local user authentication for a line.
login privilege log	Configure the logging function for privilege level increase or role switching.
memory history clear	Clear historical memory usage records.
memory low-watermark set	Enable the monitoring of memory usage threshold.

motd-banner	Enable MOTD information display for a specific line.
password	Configure a password for line-based login.
prompt	Configure a CLI prompt.
reload	Restart the device immediately.
reload at	Configure the scheduled restart function.
reload cancel	Cancel scheduled restart.
reload in	Configure the countdown restart function.
rollback running-config checkpoint	Roll back the running configurations of the device to configurations of a checkpoint.
secret	Configure an MD5/SHA-256 irreversible encrypted password for line-based login.
session	Connect to a supervisor module or service card in a virtual switching unit (VSU) environment.
session-timeout	Configure the timeout time for sessions established to a remote terminal on the current line.
show boot config	Display the saving paths and names of startup configuration files.
show calendar	Display the hardware time of the system.
show checkpoint	Display information about a single checkpoint or a summary of all checkpoints.
show clock	Display the software time of the system.
show cpu	Display CPU usage information of system tasks on control cores and non-virtual cores.
show debugging	Check whether the debugging function of the device is enabled.
show hostname	Display the host name of the device.
show language character-set	Display the character set encoding format of the device.
show line	Display configurations of a line.
show memory	Display memory information.
show memory vsd	Display memory information.

show pci-bus	Display information about devices mounted on the Peripheral Component Interconnect (PCI) bus.
show processes cpu	Display system tasks.
show processes cpu detailed	Display details about a specific task.
show reload	Display system restart configuration.
show running-config	Display the running configurations of the device system or configurations of an interface.
show service	Display the service status (enabled/disabled).
show sessions	Display information about connected telnet clients.
show startup-config	Display device configurations stored in the non-volatile random-access memory (NVRAM).
show sysmon grpc info	Display information about the gRPC function registered in the system monitoring process.
show telnet ip-block	Display information about blocked IP addresses and authentication failures.
show this	Display effective system configurations in current mode.
show usb-bus	Display information about devices mounted on the USB bus.
show version	Display the system version.
telnet	Log in to the telnet server.
username	Configure a local user account and optional authorization information.
username export	Export user information to a text file.
username import	Import user information from a text file.
write	Save system configurations (running-config) to a specific position.

1.1 banner

Function

Run the **banner** command to configure a prompt.

Run the **no** form of this command to remove this configuration.

No prompt is configured by default.

Syntax

banner { **exec** | **incoming** | **login** | **motd** | **privilege-mode** | **prompt-timeout** | **slip-ppp** } *c message c*

no banner { **exec** | **incoming** | **login** | **motd** | **privilege-mode** | **prompt-timeout** | **slip-ppp** }

Parameter Description

exec: Configures a prompt for the access to the user EXEC mode of a line.

incoming: Configures a prompt for the establishment of reverse telnet connections.

login: Configures the login banner information.

motd: Configures the message of the day (MOTD) information.

privilege-mode: Configures a prompt for the access to the privileged EXEC mode.

prompt-timeout: Configures a prompt for login authentication timeout.

slip-ppp: Configures a prompt for SLIP/PPP line connection.

c: Configures a delimiter between the command keyword and the prompt.

message: Configures prompt content, which must contain no delimiters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Any prompt configured by this command applies to all lines. Characters following the second delimiter are invalid and are discarded.

When a user logs in to the device, the MOTD information (configured using **banner motd**) and login banner information (configured using **banner login**) first appear. Upon login, the incoming prompt (**banner incoming**) is displayed in case of a reverse telnet connection and the EXEC prompt information (**banner exec**) is displayed in case of other connections.

Examples

The following example sets the prompt displayed when a user enters the user EXEC mode to **Welcome to use this device**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# banner exec $ Welcome to use this device. $
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exec-banner**
- **motd-banner**

1.2 boot config

Function

Run the **boot config** command to modify the storage path and name of the startup configuration file.

Run the **no** form of this command to remove this configuration.

The startup configuration file is stored in **Flash:/** and named **config.text** by default.

Syntax

boot config { **flash:***filename* | **usb0:***filename* }

no boot config

Parameter Description

flash: Saves the startup configuration file to the extended flash memory.

usb0: Saves the startup configuration file to Universal Serial Bus (USB) 0. This option is supported only when the device has one USB port with a USB flash drive inserted.

filename: Name of the startup configuration file.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The name of the startup configuration file must follow a slash (/), for example, **flash:/Hostname.text** or **usb0:/Hostname.text**.
- The name of the startup configuration file can be a path. If the path does not exist, the **write** command fails to save the configurations. For example, if the name of the startup configuration file is set to **flash:/Hostname/Hostname.text** or **usb0:/Hostname/Hostname.text**, in which the folders **flash:/Hostname** and **usb0:/Hostname** must exist. In master-slave mode, the paths of all devices must exist.

- To save the startup configuration file to a USB flash drive, the device must offer a USB port with a USB flash drive inserted. Otherwise, the **write** command fails to save the configurations. In master-slave mode, all devices must have a USB flash drive inserted.

Examples

The following example sets the storage path of the startup configuration file to **flash:/Hostname.text**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# boot config flash:/Hostname.text
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 calendar set

Function

Run the **calendar set** command to configure the hardware time of the system.

The default hardware time of the device is **1970-01-01 00:00:00**.

Syntax

calendar set *hh:mm:ss* [*MM* [*DD* [*YY*]]]

Parameter Description

hh:mm:ss: Hardware time of the system. *hh* indicates hours, *mm* indicates minutes, and *ss* indicates -seconds.

MM: Month. The range is from 1 to 12. If it is not specified, the current month of the system is used.

DD: Day. The range is from 1 to 31. If it is not specified, the current day of the system is used.

YY: Year. The range is from 1970 to 2037. If it is not specified, the current year of the system is used.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

- The time parameter *hour* is a mandatory field. Even if the parameter value is modified, the hour value

consistent with the current hour needs to be entered. Other parameters can be omitted if they do not need to be modified. The current system values are used for omitted parameters. For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change the month and hour but keep the values of other parameters, run the **calendar set** *12 5* command to change the current time to **2012-05-29 12:33:44**.

- The hardware time of the system is used as the Coordinated Universal Time (UTC), while the software time of the system refers to the local time of the device.
- This command is supported only by virtual switch device (VSD) 0 only. In multi-VSD mode, this command is invalid.

Examples

The following example sets the hardware time of the system to 2020-01-01 18:23:06.

```
Hostname> enable
Hostname# calendar set 18:23:06 1 1 2020
Set hardware time: 18:23:06 GMT Wed, Jan 1, 2020
Hostname#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 checkpoint

Function

Run the **checkpoint** command to configure a checkpoint.

Run the **no** form of this command to remove this configuration.

No checkpoint is configured by default.

Syntax

checkpoint [*checkpoint-name*] [**description** *description*]

no checkpoint *checkpoint-name*

Parameter Description

checkpoint-name: Checkpoint name. The value is a string of 1 to 80 characters.

description *description*: Configures checkpoint description. *description* indicates the description of the checkpoint, which cannot be longer than 80 characters.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When a checkpoint is created, the system collects and saves a copy of the current configurations. Up to 10 rollback checkpoints can be created at the same system layer.

If no checkpoint name is specified in the command, the system automatically specifies a name.

Examples

The following example configures a checkpoint that uses the default name.

```
Hostname> enable
Hostname# checkpoint
.
user-checkpoint-1 created Successfully

Done
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **clear checkpoint database**

1.5 clear checkpoint database

Function

Run the **clear checkpoint database** command to clear checkpoints and related data.

Syntax

clear checkpoint database

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear all checkpoints and their configuration file copies.

Examples

The following example clears data of all checkpoints.

```
Hostname> enable
Hostname# clear checkpoint database
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **checkpoint**

1.6 clear telnet ip-block

Function

Run the **clear telnet ip-block** command to clear entries about blocked IP addresses and authentication failures.

Syntax

clear telnet ip-block { **all** | [*ipv4-address* | *ipv6-address*] }

Parameter Description

all: Clears all entries about blocked IP addresses and authentication failures.

ipv4-address: Entries about specific blocked source IPv4 addresses and authentication failures.

ipv6-address: Entries about specific blocked source IPv6 addresses and authentication failures.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After entries about blocked IP addresses are cleared, these blocked IP addresses are awakened immediately and users using these IP addresses can log in to the device through the telnet client.

Examples

The following example clears all entries about blocked IP addresses and authentication failures.

```
Hostname> enable
Hostname# clear telnet ip-block all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 clock read-calendar

Function

Run the **clock read-calendar** command to configure the system to synchronize the software time with the hardware time.

The system is not configured to synchronize the software time with the hardware time by default.

Syntax

clock read-calendar

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

After you run this command, the system will synchronize the software time with the current hardware time according to the time zone and daylight saving time (DST) configuration of the device.

Examples

The following example configures the system to synchronize the software time with the hardware time.

```
Hostname> enable
Hostname# clock read-calendar
Set the system clock from the hardware time.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 clock set

Function

Run the **clock set** command to configure the software time of the system.

The default software time is **1970-01-01 00:00:00**.

Syntax

clock set *hh:mm*:*ss* [*MM* [*DD* [*YY*]]]

Parameter Description

hh:mm:*ss*: Software time of the system. *hh* indicates hours, *mm* indicates minutes, and *s* indicates seconds.

MM: Month. The range is from 1 to 12. If it is not specified, the current month of the system is used.

DD: Day. The range is from 1 to 31. If it is not specified, the current day of the system is used.

YY: Year. The range is from 1970 to 2037. If it is not specified, the current year of the system is used.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

The time parameter *hour* is a mandatory field. Even if the parameter value is modified, the hour value consistent with the current hour needs to be entered. Other parameters can be omitted if they do not need to be modified. The current system values are used for omitted parameters. For example, if the current software time is "2020-02-29 09:33:44" and you want to change the month and hour but keep the values of other parameters, run the **clock set** *1 2 5* command to change the current time to **2020-05-29 12:33:44**.

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

Examples

The following example sets the software time of the system to **2020-01-02 18:23:06**.

```
Hostname> enable
```

```
Hostname# clock set 18:23:06 1 2 2020
Set system clock: 18:23:06 UTC Thu, Jan 2, 2020
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 clock summer-time

Function

Run the **clock summer-time** command to configure the DST.

Run the **no** form of this command to remove this configuration.

Syntax

clock summer-time *summer-time-zone* **start** *start-month* [*week* | **last**] *start-date hh:mm* **end** *end-month* [*week* | **last**] *end-date hh:mm* [**ahead** *hours-offset* [*minutes-offset*]]

no clock summer-time

Parameter Description

summer-time-zone: DST name. The value is a case-insensitive string of 3 to 31 characters containing only English letters.

start: Specifies the start time for the DST to take effect.

start-month: Start month of the DST. The value is **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, or **December**. The value is case-insensitive, and you are allowed to enter an incomplete word, for example, **Febr** or **FebRu**.

week: Start week in the specified start month. The range is from 1 to 5.

last: Specifies the last week in a month.

start-date: Start day in the specified start month. The value is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**. The value is case-insensitive, and you are allowed to enter an incomplete word, for example, **Wed** or **WeDne**.

hh:*mm*: Specified time.

end: Specifies the end time for the DST to take effect.

end-month: End month of the DST. The value is **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**. The value is case-insensitive, and you are allowed to enter an incomplete word, for example, **Febr** or **FebRu**.

ahead: Specifies how much time that the DST is ahead of the standard time during the effective period of the DST. If it is not specified, the DST is one hour ahead of the standard time by default.

hours-offset: Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to **00:00**.

minutes-offset: Minutes ahead of the standard time. The range is from 0 to 59. If *hours-offset* is set to **0**, *minutes-offset* cannot be set to **0**.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

Examples

Assume that a time zone is named ABC and the standard time is 8:15 ahead of the UTC time, namely, GMT+08:15. The following example sets the DST to start from the first Saturday in February to the third Monday in May, and 01:20 ahead of the standard time. In this case, the DST is 09:35 ahead of the UTC time, but non-DST time is still 08:15 ahead of the UTC time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
Hostname(config)# end
Hostname# show clock
16:39:16 ABC Wed, Feb 29, 2012
Hostname# show calendar
08:24:35 GMT Wed, Feb 29, 2012
Hostname# configure terminal
Hostname(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30
ahead 1 20
*May 10 03:45:58: %SYS-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday
at 2:00 TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at
18:30, ahead 1 hour 20 minute
Hostname(config)# end
Hostname# show clock
18:00:08 TZA Wed, Feb 29, 2012
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 clock timezone

Function

Run the **clock timezone** command to configure a time zone.

Run the **no** form of this command to remove this configuration.

The UTC time is set for all time zones by default.

Syntax

clock timezone *timezone hours-offset* [*minutes-offset*]

no clock timezone

Parameter Description

timezone: Time zone name. The value is a case-insensitive string of 3 to 31 characters containing only English letters.

hours-offset: Hours of the specified time difference. It indicates the time that the time zone is faster or slower than the hardware time (UTC time). The range is from –12 to 12. A negative number indicates that the time zone is slower than the hardware time, while a positive number indicates that the time zone is faster than the hardware time. If the time zone is slower than the UTC time, add "–" before *hours-offset*.

minutes-offset: Minutes of the specified time difference. The range is from 0 to 59.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

Examples

The following example sets the time zone name to **CST** and the software time to be 8 hours faster than the hardware time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)
Hostname# show clock
18:00:17 CST Wed, Dec 5, 2012
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 clock update-calendar

Function

Run the **clock update-calendar** command to configure the system to synchronize the hardware time with the software time.

The system is not configured to synchronize the hardware time with the software time by default.

Syntax

clock update-calendar

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

- This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.
- After you configure this command, the device will synchronize the hardware time with the current software time according to the time zone and DST configuration of the device.

Examples

The following example configures the device to synchronize the hardware time with the software time.

```
Hostname> enable
Hostname# clock update-calendar
Set the hardware time from the system clock.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 configure

Function

Run the **configure** command to enter the global configuration mode.

Syntax

configure [**terminal**]

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enters the global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 cpu high-watermark set

Function

Run the **cpu high-watermark set** command to configure the maximum threshold for the total CPU usage of all control cores and enable CPU usage monitoring.

Run the **no** form of this command to disable CPU usage monitoring.

Run the **default** form of this command to restore the default configuration.

The default CPU usage range is from **75%** to **85%**.

Syntax

cpu high-watermark set [[**up** *up-value*] [**down** *down-value*]]

no cpu high-watermark set

default cpu high-watermark set

Parameter Description

watermark-up-value: Upper limit of the CPU usage. The range is from 1% to 99%.

watermark-down-value: Lower limit of the CPU usage. The range is from 1% to 99%.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.
- You can use this command to configure the maximum threshold for CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the allowed threshold range, the system prints a prompt.

Examples

The following example enables CPU usage monitoring and sets the lower limit of the CPU usage to 70% and upper limit to 90%.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu high-watermark set up 90 down 70
Open cpu watermark monitor
Set system cpu high-watermark up 90%, down 70%
```

Notifications

When the CPU usage range is from 85% to 91% and the CPU usage exceeds the upper limit, the following alarm information is printed:

```
*Mar 11 09:59:01: %SYSMON-4-CPU_WATERMARK_HIGH: Warning! System cpu usage above high watermark(1%), current cpu usage 92%
```

```
*Mar 11 09:59:01: %SYSMON-4-CPU_WATERMARK_HIGH: TOP 1: pid is 7368, task name is
bcmL2X.0, run in core 0, cpu usage  4.2%
*Mar 11 09:59:01: %SYSMON-4-CPU_WATERMARK_HIGH: TOP 2: pid is 7369, task name is
bcmCNTR.0, run in core 1, cpu usage  2.7%
*Mar 11 09:59:01: %SYSMON-4-CPU_WATERMARK_HIGH: TOP 3: pid is 7561, task name is
monitor_procps, run in core 0, cpu usage  1.0%
*Mar 11 09:59:05: %SYSMON-4-CPU_WATERMARK_HIGH: (*2/0) Warning! System cpu usage above
high watermark(1%), current cpu usage 92%
*Mar 11 09:59:05: %SYSMON-4-CPU_WATERMARK_HIGH: (*2/0) TOP 1: pid is 7368, task name
is bcmL2X.0, run in core 0, cpu usage  4.2%
*Mar 11 09:59:05: %SYSMON-4-CPU_WATERMARK_HIGH: (*2/0) TOP 2: pid is 7369, task name
is bcmCNTR.0, run in core 1, cpu usage  2.7%
*Mar 11 09:59:05: %SYSMON-4-CPU_WATERMARK_HIGH: (*2/0) TOP 3: pid is 7561, task name
is monitor_procps, run in core 0, cpu usage  1.0%
```

When the CPU usage is below the lower limit, the following alarm clearance information is printed:

```
*Mar 11 10:01:12: %SYSMON-5-CPU_WATERMARK: Withdraw warning! System cpu usage below
high watermark(75%), current cpu usage 20%
*Mar 11 10:01:18: %SYSMON-5-CPU_WATERMARK: (*2/0) Withdraw warning! System cpu usage
below high watermark(75%), current cpu usage 20%
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

-

1.14 disconnect

Function

Run the **disconnect** command to close a suspended telnet client session.

Syntax

disconnect *session-id*

Parameter Description

session-id: ID of the suspended telnet client session.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

You can run this command with a telnet client session ID specified to close the specified telnet client session.

Examples

The following example closes telnet client session 1.

```
Hostname> enable
Hostname# disconnect 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show sessions**

1.15 do telnet

Function

Run the **do telnet** command to log in to the telnet server.

Syntax

do telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

Parameter Description

oob: Connects to a remote telnet server through out-of-band communication (over the MGMT port typically).

hostname: Host name of the telnet server.

ipv4-address: IPv4 host address of the telnet server.

ipv6-address: IPv6 host address of the telnet server.

port-number: TCP port number of the telnet server. The range is from 0 to 65535, and the default value is **23**.

/source: Specifies the source IP address or source interface used by the telnet client.

ip *ipv4-address*: Specifies the source IPv4 address used by the telnet client.

ipv6 *ipv6-address*: Specifies the source IPv6 address used by the telnet client.

interface *interface-type interface-name*: Specifies the source interface used by the telnet client. *interface-type interface-name* indicates the specified interface type and ID.

via *mgmt-name*: Specifies the MGMT port used by the telnet client for the **oob** parameter. *mgmt-name* indicates the MGMT port number.

Command Modes

User EXEC mode, privileged EXEC mode, and interface configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example sets the IPv4 address of the telnet server to **192.168.1.1**, the TCP port number to the default value, the source interface to **Gi 0/1**, and the VRF table to **vpn1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# do telnet 192.168.1.1 /source interface gigabitethernet 0/1 /vrf
vpn1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 enable

Function

Run the **enable** command to enter the privileged EXEC mode or switch a role.

Syntax

enable [[*privilege-level*] | [**role** *role-name*]]

Parameter Description

privilege-level: Privilege level.

role-name: Role name.

Command Modes

User EXEC mode

Default Level

0

Usage Guidelines

This command is used to switch from the user EXEC mode to the privileged EXEC mode by default. If privilege level is specified, the current privilege level is raised to the specified level.

When the RBAC function is enabled, this command can be used to switch the terminal role. If no role is specified, the system switches to role **network-admin** by default.

Examples

The following example raises the current privilege level to level 14.

```
Hostname> enable 14
Password:
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show privilege** (Line)

1.17 enable default role

Function

Run the **enable default role** command to configure the default role for running the **enable** commands.

Run the **no** form of this command to restore the role for running the **enable** commands to the default role.

The default role for running **enable** commands is **network-admin**.

Syntax

enable default role *role-name*

no enable default role

Parameter Description

role-name: Role name.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- The **enable** commands include **enable** (for role switching), **enable password**, and **enable secret**. If no role is specified, these three commands are used to set the role configured by this command.
- This command is set only when the RBAC function is enabled.

Examples

The following example sets the role for running the **enable** commands to **network-operator**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable default role network-operator
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 enable password

Function

Run the **enable password** command to configure passwords for different privilege levels.

Run the **no** form of this command to remove this configuration.

Syntax

enable password { [**level** *password-level*] | [**role** *role-name*] } { [**0**] *password* | **7** *encrypted-password* }

no enable password { [**level** *password-level*] | [**role** *role-name*] }

Parameter Description

password-level: Privilege level of a user.

role-name: Role name.

0: Sets the entered password to a plaintext string.

password: Plaintext password used to enter the configuration layer of the privileged EXEC mode. The value is a string of 1 to 126 characters.

7 *encrypted-password*: Configures the entered password as a ciphertext string.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

A valid password is defined as follows:

- It contains 1 to 26 characters including uppercase letters, lowercase letters, and digits.
- Preamble spaces are allowed in front of the password, but are ignored. Intermediate and trailing spaces are recognized.

Generally, the encryption type is specified only when a password encrypted by the device is copied and pasted.

When the RBAC function is enabled and no role is specified, this command is used to set a password for role **network-admin** by default.

Caution

- Encrypted passwords cannot be restored but can be reconfigured.
- If you specify an encryption type but enter a plaintext password, you are not allowed to enter the privileged EXEC mode again.

Examples

The following example sets a password of role **network-operator** to the plaintext string **passwword10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable password password10
Hostname(config)# enable password role network-operator
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 enable secret

Function

Run the **enable secret** command to configure secure encrypted passwords for different privilege levels.

Run the **no** form of this command to remove this configuration.

Syntax

enable secret { [**level** *secret-level*] | [**role** *role-name*] } { [**0**] *password* | **5** *encrypted-secret* }

no enable secret { [**level** *secret-level*] | [**role** *role-name*] }

Parameter Description

secret-level: Privilege level of a user.

role-name: Role name.

0: Sets the output password to a plaintext string.

password: Plaintext password used to enter the configuration layer of the privileged EXEC mode. The value is a string of 1 to 126 characters.

5 *encrypted-secret*: Configures the password encryption mode. **5** indicates that a password encrypted using the MD5 irreversible encryption algorithm is saved as an encrypted password.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

Authentication passwords configured using the **Enable** command are classified into passwords and secrets.

- Passwords are simple encrypted passwords set for privilege levels 1 to 15.
- Secrets are secure encrypted passwords set for privilege levels 1 to 15.

Passwords must be stored in encryption mode. Passwords are simply encrypted, and secrets are securely encrypted.

If a privilege level has both a password and a secret, the password does not take effect.

If you configure a password for a non-15 level, a warning is displayed and the password is automatically converted into a secret.

If the password and secret set for level 15 are the same, a warning is displayed.

When the RBAC function is enabled and no role is specified, this command is used to set a password for role **network-admin** by default.

Examples

The following example sets the secure encrypted password to the plaintext string **secret10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable secret 0 secret10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 enable service

Function

Run the **enable service** command to enable a specified service.

Run the **no** form of this command to disable the specific service.

The Simple Network Management Protocol (SNMP) agent service is enabled and the telnet server, Secure Shell (SSH) server, and Web server services are disabled by default.

Syntax

enable service { **ssh-server** | **telnet-server** | **web-server** [**http** | **https** | **all**] | **snmp-agent** }

no enable service { **ssh-server** | **telnet-server** | **web-server** [**http** | **https** | **all**] | **snmp-agent** }

Parameter Description

ssh-server: Enables the SSH server service.

telnet-server: Enables the telnet server service.

web-server [**http** | **https** | **all**]: Enables the Web server service. **http** indicates that only the Hypertext Transfer Protocol (HTTP) service is enabled. **https** indicates that only the Hypertext Transfer Protocol Secure (HTTPS) service is enabled. **all** indicates that both the HTTP and HTTPS services are enabled.

snmp-agent: Enables the SNMP agent service.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the **ssh-server** command is run, both the IPv4 and IPv6 services of the SSH server are enabled.

When the **telnet-server** command is run, both the IPv4 and IPv6 services of the telnet server are enabled.

When the **web-server** [**http** | **https** | **all**] command is run, both the IPv4 and IPv6 services of the web server are enabled.

When the **snmp-agent** command is run, both the IPv4 and IPv6 services of the SNMP agent are enabled.

Examples

The following example enables the SSH server service.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# enable service ssh-server
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 end

Function

Run the **end** command to exit the current mode and return to the privileged EXEC mode.

Syntax

end

Parameter Description

N/A

Command Modes

All modes except the privileged EXEC mode

Default Level

0

Usage Guidelines

In any mode except the privileged EXEC mode, you can run the **end** command to exit the current mode and return to the privileged EXEC mode.

Examples

The following example exits from the line configuration mode and returns to the privileged EXEC mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# end
Hostname#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 exec-banner

Function

Run the **exec-banner** command to enable EXEC prompt information display for a specific line.

Run the **no** form of this command to remove this configuration.

EXEC prompt information display is enabled for all lines by default.

Syntax

exec-banner

no exec-banner

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

If the **banner exec** command is configured on the device, EXEC prompts are displayed for all lines by default. To disable EXEC prompt information for a specific line, run the **no exec-banner** command.

Caution

This command does not support **banner incoming**. That is, if **banner incoming** is configured for the device, incoming prompts are displayed for reverse telnet connections of all lines. You cannot disable the incoming prompts on a specific line.

Examples

The following example disables welcome information display for line 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
```

```
Hostname(config-line)# no exec-banner
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- banner banner motd 1

1.23 exec-timeout

Function

Run the **exec-timeout** command to set the connection timeout time of the device on a line.

Run the **no** form of this command to remove this configuration.

The default connection timeout time of the device on a line is 10 minutes.

Syntax

exec-timeout *exec-timeout-minutes* [*exec-timeout-seconds*]

no exec-timeout

Parameter Description

exec-timeout-minutes: Timeout time, in minutes. The range is from 0 to 35791.

exec-timeout-seconds: Timeout time, in seconds. The range is from 0 to 2147483.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

The connection timeout time of the device on a line is the sum of the configured minutes and seconds. If a connection does not have any input or output information within the timeout time, the device interrupts this connection and restores the line to the idle state.

Examples

The following example sets the connection timeout time of the device on VTY 0 to 5 minutes and 30 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
```

```
Hostname(config-line)# exec-timeout 5 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 execute

Function

Run the **execute** command to run commands in the batch file.

Syntax

execute { [**flash**:] *filename* }

Parameter Description

filename: Path where the batch file is stored.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When the **execute** command is run, the device reads and executes character strings in the batch file line by line. When the file contains multiple commands, a line feed is required between different commands.

Examples

The following example uses the **execute** command to run commands in the batch file and sets the IP address of interface GigabitEthernet 0/1 to **192.168.21.158/24**.

```
Hostname> enable
Hostname# execute flash:mybin/config.text
executing script file mybin/config.text ......
executing done
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet gigabitethernet 0/1
Hostname(config-if-gigabitethernet 0/1)# ip address 192.168.21.158 24
Hostname(config-if-gigabitethernet 0/1)# end
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 exit

Function

Run the **exit** command to exit the configuration mode and return to the upper-level mode or exit the command line interface (CLI) from the privileged EXEC mode.

Syntax

exit

Parameter Description

N/A

Command Modes

All modes

Default Level

0

Usage Guidelines

N/A

Examples

The following example exits the line configuration mode and returns to the upper-level mode (global configuration mode).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# exit
Hostname(config)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 Help

Function

Run the **help** command to display a brief description of the help system.

Syntax

Help

Parameter Description

N/A

Command Modes

All modes

Default Level

1

Usage Guidelines

During configuration, you can use a question mark (?) to display all commands in the current configuration mode or keywords and variables of parameters carried in a command.

Examples

The following example displays brief description of the help system.

```
Hostname> enable
Hostname# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

The following example displays all commands that can be run in interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-gigabitethernet 0/1)# ?
Interface configuration commands:
  arp            ARP interface subcommands
  bandwidth       Set bandwidth informational parameter
  carrier-delay    Specify delay for interface transitions
  dampening       Enable event dampening
  default         Set a command to its defaults
  description     Interface specific description
  dldp           Exec data link detection command
  duplex          Configure duplex operation
  efm            Config efm for an interface
  end            Exit from interface configuration mode
  exit           Exit from interface configuration mode
  expert          Expert extended ACL
  flowcontrol     Set the flow-control value for an interface
  full-duplex     Force full duplex operation
  global          Global ACL
  gvrp           GVRP configure command
  half-duplex     Force half duplex operation
  help           Description of the interactive help system
  ip             Interface Internet Protocol config commands
  ipv6           Internet Protocol Version 6
  isis           Intermediate System - Intermediate System (IS-IS)
  l2             Config L2 attribute
  label-switching  Enable interface process mpls packet
  lacp           LACP interface subcommands
  lldp           Link Layer Discovery Protocol
  load-interval    Specify interval for load calculation for an interface
  mac            Mac extended ACL
  mac-address     Set mac-address
  mpls           Multi-Protocol Label Switching
  mtu            Set the interface Maximum Transmission Unit (MTU)
  no             Negate a command or set its defaults
  ntp            Configure NTP
  port-group      Aggregateport/port bundling configuration
  redirect        Redirect packets
  rmon           Rmon command
  security        Configure the Security
  show           Show running system information
  shutdown        Shutdown the selected interface
  snmp           Modify SNMP interface parameters
  speed          Configure speed operation
  switchport      Set switching mode characteristics
```

```
 vrf            Multi-af VPN Routing/Forwarding parameters on the interface
 vrrp           VRRP interface subcommands
 xconnect        Xconnect commands
```

The following example displays keywords and variables of parameters carried in the **access-list 1 permit** command.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit ?
 A.B.C.D  Source address
 any     Any source host
 host    A single source host
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 hostname

Function

Run the **hostname** command to specify or modify the host name of the device.

Run the **no** form of this command to restore the host name of the device to the default value.

The default host name is **Ruijie**.

Syntax

hostname *hostname*

Parameter Description

hostname: Host name of the device. The value is a string of up to 63 characters containing only letters, digits, and hyphens (-).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The host name is used to identify a device and acts as the username of the local device in dialing and Challenge-Handshake Authentication Protocol (CHAP) authentication scenarios.

Examples

The following example sets the host name of the device to **Beijing_Hostname**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# hostname Beijing_Hostname
Beijing_Hostname(config)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ip telnet access-class

Function

Run the **ip telnet access-class** command to configure an access control list (ACL) for the telnet server.

Run the **no** form of this command to remove this configuration.

Syntax

ip telnet access-class { *acl-number* | *acl-name* }

no ip telnet access-class

Parameter Description

acl-number: ACL ID. Value range:

Standard ACLs for IP addresses: 1–99 or 1300–1999; extended ACLs for IP addresses: 100–199 or 2000–2699; extended ACLs for MAC addresses: 700–799; expert extended ACLs: 2700–2899

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In line configuration mode, an ACL applies only to a specific line. However, an ACL of the telnet server is effective to all connections to the telnet server.

Examples

The following example filters all connections to the telnet server by the keyword **testv4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip telnet access-class testv4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ip telnet ip-block

Function

Run the **ip telnet ip-block** command to configure the maximum number of consecutive authentication failures, beyond which an IP address is blocked on the telnet server, and to specify the period for awakening the blocked IP address.

Run the **no** form of this command to remove this configuration.

The IP address blocking function is enabled on the telnet server by default. The maximum number of consecutive authentication failures is 6, the period for resetting the authentication failure count is 5 minutes, and blocked IP addresses are awakened 5 minutes after their blocking.

Syntax

ip telnet ip-block { **disable** | **failed-times** *failed-times* **period** *period-time* | **reactive** *reactive-period-time* }

no ip telnet ip-block { **disable** | **failed-times** *failed-times* **period** *period-time* | **reactive** *reactive-period-time* }

Parameter Description

disable*:* Disables the IP address blocking function of the telnet server.

failed-times *failed-times*: Configures the maximum number of consecutive authentication failures, beyond which an IP address is blocked. The range is from 1 to 10. The default value is **6**.

period *period-time*: Configures the period for counting the number of consecutive authentication failures, in minutes. The range is from 1 to 120. The default value is **5**.

reactive *reactive-period-time*: Configures the period for awakening blocked IP addresses, in minutes. The range is from 1 to 1000. The default value is **5**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the IP address blocking function is enabled and the number of consecutive authentication failures for telnet login reaches the configured limit in the authentication failure count period, the source IP address blocking is triggered. That is, the telnet client that uses this source IP address is not allowed to log in to the device to prevent the device from being attacked. Only after the period for awakening blocked IP addresses expires, the telnet client can log in to the device.

Examples

The following example sets the maximum number of consecutive authentication failures, beyond which an IP address is blocked on the telnet server to **3**, the period for resetting the authentication failure count to 3 minutes, and the period for awakening blocked IP addresses to 3 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip telnet ip-block failed-times 3 period 3
Hostname(config)# ip telnet ip-block reactive 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 ip telnet source-interface

Function

Run the **ip telnet source-interface** command to specify the IP address of an interface as the source IP address of a telnet connection.

Run the **no** form of this command to remove this configuration.

Syntax

ip telnet source-interface *interface-type interface-name*

Parameter Description

source-interface *interface-type interface-name*: Specifies the IP address configured on an interface as the source IP address of a telnet connection. *interface-type interface-name* indicates the interface type and interface ID.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When you connect to a telnet server through telnet, the IP address configured by this command is used if no source interface or source IP address is specified for this connection.

Examples

The following example specifies the IP address of interface Loopback 1 as the source IP address of the global telnet connection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip telnet source-interface Loopback 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 ipv6 telnet access-class

Function

Run the **ipv6 telnet access-class** command to configure an IPv6 ACL for a telnet server.

Run the **no** form of this command to remove this configuration.

Syntax

ipv6 telnet access-class { *acl-number* | *ipv6-acl-name* }

no ipv6 telnet access-class

Parameter Description

acl-number: ACL ID. Value range:

Standard ACLs for IP addresses: 1–99 or 1300–1999; extended ACLs for IP addresses: 100–199 or 2000–2699; extended ACLs for MAC addresses: 700–799; expert extended ACLs: 2700–2899

ipv6-acl-name: IPv6 ACL name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure an IPv6 ACL for all connections to a telnet server. In line configuration mode, an IPv6 ACL applies only to a specific line. However, an IPv6 ACL of a telnet server is effective to all connections to the telnet server.

Examples

The following example filters all connections to the telnet server by the keyword **testv6**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 telnet access-class testv6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 lock

Function

Run the **lock** command to set a temporary password on a terminal to lock the terminal CLI to prevent access while keeping the session.

Syntax

lock

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

Before running this command, run the **lockable** command in line configuration mode to enable the terminal locking feature. After running this command, configure a temporary password for unlocking.

Examples

The following example sets the temporary password for locking the CLI of virtual terminal 1 to **<password>**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# lockable
Hostname(config-line)# end
Hostname# lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lockable**

1.33 lockable

Function

Run the **lockable** command to enable the locking feature for terminals connected to the current line.

Run the **no** form of this command to disable this feature.

The locking of terminals connected to the current line is disabled by default.

Syntax

lockable

no lockable

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

1

Usage Guidelines

After you enable the terminal locking feature for a line by running this command, you can run the **lock** command in EXEC mode to lock terminals.

Examples

The following example enables terminal locking on the console port and locks the console.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# lockable
Hostname(config-line)# end
Hostname# lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lock**

1.34 login

Function

Run the **login** command to configure simple login password verification for a line.

Run the **no** form of this command to remove this configuration.

The simple login password verification function is disabled for the console line and enabled for the virtual terminal lines by default.

Syntax

login

no login

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

This command is used to configure simple password verification during login authentication, that is, the password configured for the virtual terminal or console port, only when the authentication, authorization, and accounting (AAA) service is disabled.

Examples

The following example configures login password verification for virtual terminal 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no aaa new-model
Hostname(config)# line vty 0
Hostname(config-line)# password 0 password10
Hostname(config-line)# login
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **no aaa new-model** (Security/AAA)

1.35 login access non-aaa

Function

Run the **login access non-aaa** command to enable non-AAA authentication for a line when the AAA service is enabled.

Run the **no** form of this command to disable non-AAA authentication.

When AAA is enabled, non-AAA authentication is disabled by default.

Syntax

login access non-aaa

no login access non-aaa

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To perform non-AAA authentication for a line when AAA is enabled, run this command. The configuration is valid for all terminals.

Examples

The following example configures local user authentication for virtual terminal 4 when AAA is enabled.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# login access non-aaa
Hostname(config)# aaa new-model
Hostname(config)# line vty 4
Hostname(config-line)# login local
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa new-model** (Security/AAA)

1.36 login local

Function

Run the **login local** command to configure local user authentication for a line.

Run the **no** form of this command to remove this configuration.

When the AAA service is disabled, local user authentication is not configured for a line by default.

Syntax

login local

no login local

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

This command is valid only when the AAA service is disabled. The local user refers to the user configured by running the **username** command.

Examples

The following example configures local user authentication for virtual terminal 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no aaa new-model
Hostname(config)# username test password 0 password10
Hostname(config)# line vty 0
Hostname(config-line)# login local
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **username**

1.37 login privilege log

Function

Run the **login privilege log** command to configure the logging function for privilege level increase or role switching.

Run the **no** form of this command to remove this configuration.

The prompt output function is disabled by default.

Syntax

login privilege log

no login privilege log

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can use this command to monitor privilege level increase or role switching of terminal users. The configuration is valid for all terminals.

Examples

The following example enables the logging function of privilege level increase.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# login privilege log
```

If the privilege level increase fails, the device prints the following log:

```
Hostname>enable 10
Password:
Password:
Password:
% Access denied
Hostname>
*Sep 10 11:34:19: %SYS-PRIV_AUTH_FAIL: Authentication to privilege level 10 from
console failed
```

If the privilege level increase is successful, the device prints the following log:

```
Hostname>enable 10
Password:
Hostname#
```

```
*Sep 10 11:34:20: %SYS-PRIV_AUTH_SUCCESS: Authentication to privilege level 10 from
console success
```

If the logging and RBAC functions are enabled and role switching to **network-admin** fails, the device prints the following log

```
Hostname> enable
Hostname# enable role network-admin
Password:
Password:
Password:
% Access denied
Hostname>
*Sep 10 11:34:19: %SYS-PRIV_AUTH_FAIL: Authentication to role network-admin from
console failed
```

If the logging and RBAC functions are enabled and role switching to **network-admin** is successful, the device prints the following log:

```
Hostname> enable
Hostname# enable role network-admin
Password:
Hostname#
*Sep 10 11:34:20: %SYS-PRIV_AUTH_SUCCESS: Authentication to role network-admin from
console success
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 memory history clear

Function

Run the **memory history clear** command to clear historical memory usage records.

Syntax

memory history clear [**one-forth** | **half** | **all**]

Parameter Description

one-forth: Clears 25% of historical information.

half: Clears half of historical information.

all: Clears all historical information.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example clears half of historical memory usage records.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# memory history clear half
2 out of 5 records in the history table to be cleared...
Clear done !
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 memory low-watermark set

Function

Run the **memory low-watermark set** command to enable the monitoring of memory usage threshold.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The default memory usage threshold is **90%**.

Syntax

memory low-watermark set *memory-threshold*

no memory low-watermark set

default memory low-watermark set

Parameter Description

memory-threshold: Memory usage threshold. The range is from 1% to 100%.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the memory usage threshold to **80%** and enables the monitoring function of memory usage.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# memory low-watermark set 80
```

Notifications

When the memory usage is higher than the threshold, the system prints the following alarm information:

```
*Mar 11 09:58:45: %SYSMON-4-MEM_HIGH: The current memory usage 90%
*Mar 11 09:58:45: %SYSMON-4-MEM_HIGH: (*2/0) The current memory usage 90%
```

When the memory usage is lower than the threshold, the system prints the following alarm clearance information:

```
*Mar 11 10:11:17: %SYSMON-5-MEM_RECOVER: The current memory usage 58%
*Mar 11 10:11:16: %SYSMON-5-MEM_RECOVER: (*2/0) The current memory usage 58%
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 motd-banner

Function

Run the **motd-banner** command to enable MOTD information display for a specific line.

Run the **no** form of this command to remove this configuration.

MOTD information display is enabled for all lines by default.

Syntax

motd-banner

no motd-banner

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

If this command is configured on the device, MOTD information is displayed for all lines by default. To disable MOTD information display for a specific line, run the **no** form of this command.

This command is invalid for **banner incoming**. That is, if **banner incoming** is configured for the device, incoming prompts are displayed for reverse telnet connections of all lines. The incoming prompt display cannot be disabled for a specific line.

Examples

The following example disables MOTD information display for virtual terminal 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# no motd-banner
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **banner**

1.41 password

Function

Run the **password** command to configure a password for line-based login.

Run the **no** form of this command to remove this configuration.

Syntax

password { [**0**] *password* | **7** *encrypted-password* }

no password

Parameter Description

0: Configures a plaintext password.

password: Plaintext password for a line. The string length range is from 1 to 25.

7 *encrypted-password*: Configures the entered password as a ciphertext string.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the password for line-based login to **password10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# password password10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 prompt

Function

Run the **prompt** command to configure a CLI prompt.

Run the **no** form of this command to remove this configuration.

No CLI prompt is configured by default and the system name is used as the prompt. In this case, the prompt changes with the system name.

Syntax

prompt *prompt-string*

no prompt

Parameter Description

prompt-string: Command prompt. The value is a string of up to 32 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

CLI prompts take effect only in EXEC mode.

Examples

The following example sets the CLI prompt to **CustomerA**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# prompt CustomerA
Hostname(config)# end
CustomerA
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 reload

Function

Run the **reload** command to restart the device immediately.

Syntax

reload

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

If the device is in a cluster, all in-service devices in the cluster will be restarted immediately after this command is run.

Examples

The following example restarts the device immediately.

```
Hostname> enable
Hostname# reload
Reload system?(Y/N) y
Hostname# [667365.374976] %SYS-0-REBOOT: Rebooting by job:
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 reload at

Function

Run the **reload at** command to configure the scheduled restart function.

The scheduled restart function is not configured by default.

Syntax

reload at *hh*:*mm*:*ss* [*MM* [*DD* [*YY*]]]

Parameter Description

hh:*mm*:*ss*: Scheduled restart time. *hh* indicates hours, *mm* indicates minutes, and *ss* indicates seconds.

MM: Month. The range is from 1 to 12. If it is not specified, the current month of the system is used.

DD: Day. The range is from 1 to 31. If a day does not exist in a month, the day is moved to the following day. If it is not specified, the current day of the system is used.

YY: Year. The range is from 1970 to 2037. If it is not specified, the current year of the system is used.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

If the device is in a cluster, all in-service devices in the cluster will be restarted at the scheduled time after this command is run.

Examples

The following example restarts the device at 12:00:00 August 21, 2019.

```
Hostname> enable
Hostname# reload at 12:00:00 8 21 2019
% Set reload ok.
% Reload scheduled for 12:00:00 Beijing Wed Aug 21 2019 (in 45 hours and 15 minutes),
will be cancled after system halt.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 reload cancel

Function

Run the **reload cancel** command to cancel scheduled restart.

Syntax

reload cancel

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example cancels scheduled restart.

```
Hostname> enable
Hostname# reload cancel
*Aug 19 14:45:44: %SYSMON-RELOAD: Scheduled reload cancelled.
% Scheduled reload cancelled.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 reload in

Function

Run the **reload in** command to configure the countdown restart function.

The countdown restart function is not configured by default.

Syntax

reload in { [*hh* :] *mm*] }

Parameter Description

[*hh* :] *mm*: Countdown restart time. *hh* indicates hours. If it is not specified, it is set to **0** by default. *mm* indicates minutes.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

If the device is in a cluster, all in-service devices in the cluster will be restarted according to the countdown timer after this command is run.

Examples

The following example configures the device to restart after 1 hour and 20 minutes.

```
Hostname> enable
```

```
Hostname# reload in 1:20
% Set reload ok.
% Reload scheduled for 16:05:38 Beijing Mon Aug 19 2019 (in 1 hour and 20 minutes),
will be cancled after system halt.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 rollback running-config checkpoint

Function

Run the **rollback running-config checkpoint** command to roll back the running configurations of the device to configurations of a checkpoint.

Syntax

rollback running-config checkpoint *checkpoint-name* [**display-differences** | **ignore-results**]

Parameter Description

checkpoint-name: Checkpoint name. The value is a string of 1 to 80 characters.

display-differences: Displays configuration differences upon rollback. Configuration differences are displayed by default.

ignore-results: Ignores the execution results without configuration differences displayed upon rollback.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to roll back the running configurations of the device to configurations of a specific checkpoint. Only one user can create checkpoints and roll back configurations on a device at a time. When the **display-differences** and **ignore-results** parameters are not configured, configuration differences are displayed.

Before rollback, you can run the **show running-config** command to display the current configurations. After rollback, you can run the **show running-config** command to check whether the checkpoint configurations are applied.

If an "Increased configuration:" message is displayed after rollback, configurations increase from the checkpoint configurations. This is because some commands cannot be reversed or fail to be reversed. For details, see the command manuals of specific functions, and manually reserve these commands.

If a "Decreased configuration:" message is displayed after rollback, configurations decrease from the checkpoint configurations. This is because some commands fail to be executed during rollback. For details, see the command manuals of specific functions, and manually run these commands.

Examples

The following example rolls back the running configurations to configurations of checkpoint user-1.

```
Hostname> enable
Hostname# rollback running-config checkpoint user-checkpoint-1 ignore-results
...
Rollback configuration successfully.
```

Notifications

If configuration rollback is successful, the following notification is displayed:

```
...
Rollback configuration successfully.
```

If configuration differences exist upon rollback, the following notification is displayed:

```
..
Rollback configuration completed.

Increased configuration:
+ spanning-tree mode rstp          //The plus sign (+) indicates increased
configuration commands from the checkpoint configurations.
Decreased configuration:
- username admin password admin     // The minus sign (-) indicates decreased
configuration commands from the checkpoint configurations.
```

If configuration rollback fails, the following notification is displayed:

```
...
Rollback configuration failed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show running-config**

1.48 secret

Function

Run the **secret** command to configure an MD5/SHA-256 irreversible encrypted password for line-based login.

Run the **no** form of this command to remove this configuration.

No encrypted password is configured for line-based login by default.

Syntax

secret { [**0**] *password* | **5** *encrypted-secret* }

no secret

Parameter Description

0: Specifies a plaintext password. After it is configured, MD5 irreversible encryption is used.

password: Plaintext password for line-based login. The value is a string of 1 to 25 characters.

5 *encrypted-secret*: **5** specifies a password encrypted using the MD5 irreversible encryption algorithm. The password is saved as an encrypted password after configuration.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

This command is used to configure an MD5/SHA-256 irreversible encrypted password for authenticating remote users who attempt to log in to the device through a line. When both a password and secret are configured for a line, the secret is preferentially matched during user login. If secret matching fails, the password is matched. If the matching of both the secret and password fails, the login fails.

Caution

- If the value **5** is selected for the encryption type, the entered ciphertext password must contain 24 characters with the 1st, 3rd, and 8th characters set to the dollar sign ($).

Examples

The following example configures an MD5 irreversible encrypted password for login through virtual terminal 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# algorithm-type md5
Hostname(config-line)# secret secretvty0
```

Notifications

After this password is configured, virtual terminal 0 uses MD5 irreversible encryption for the password and the effect is as follows:

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **algorithm-type**

1.49 session

Function

Run the **session** command to connect to a supervisor module or service card in a virtual switching unit (VSU) environment.

Syntax

session { **master** | **device** *device-number* }

session { **device** *device-number* | **master** }

Parameter Description

master: Specifies the slave device to connect to the master device or the slave supervisor module to connect to the master supervisor module.

device *device-number*: Specifies the device ID. *device-number* indicates the device ID.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

This command is used in a multi-node VSU environment.

Examples

The following example specifies the slave device to connect to the master device in a VSU environment.

```
Hostname> enable
Hostname# session master
```

The following example connects sessions to device 1 in a multi-node VSU environment.

```
Hostname> enable
Hostname# session device 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 session-timeout

Function

Run the **session-timeout** command to configure the timeout time for sessions established to a remote terminal on the current line.

Run the **no** form of this command to remove this configuration.

The default session timeout time is 0 minute for remote terminals. That is, the sessions never time out.

Syntax

session-timeout *session-timeout-time* [**output**]

no session-timeout

Parameter Description

session-timeout-time: Timeout time of sessions to a remote terminal in minutes. The range is from 0 to 35791. **0** indicates that a session never times out.

output: Specifies output data as a timeout criterion.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

If a session established to a remote terminal on a line does not have any input or output within the specified time upon configuration of this command, the device closes this session and restores the line to the idle state.

Examples

The following example sets the timeout time of sessions on virtual terminal 0 to 5 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# session-timeout 5 output
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 show boot config

Function

Run the **show boot config** command to display the saving paths and names of startup configuration files.

Syntax

show boot config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the saving path and name of startup configuration file.

```
Hostname> enable
Hostname# show boot config
Boot config file: [flash:/Hostname.text]
```

Table 1-1 Output Fields of the show boot config Command

Field	Description
Boot config file	Specifies the saving path and name of startup configuration file.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 show calendar

Function

Run the **show calendar** command to display the hardware time of the system.

Syntax

show calendar

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the hardware time of the system.

```
Hostname> enable
Hostname# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

Table 1-2 Output Fields of the show calendar Command

Field	Description
21:57:48	Hours, minutes, and seconds
GMT	Time zone
Sun	Week
Feb 28	Month and day
2012	Year

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.53 show checkpoint

Function

Run the **show checkpoint** command to display information about a single checkpoint or a summary of all checkpoints.

Syntax

show checkpoint { *checkpoint-name* [**all**] | **summary** }

Parameter Description

checkpoint-name: Checkpoint name. The value is a string of 1 to 80 characters.

all: Displays all information about a specified checkpoint.

summary: Displays a summary of all checkpoints.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays a summary of all checkpoints.

```
Hostname> enable
Hostname# show checkpoint summary
User Checkpoint Summary
--------------------------------------------------------------------------------
1) clo:
Created at 11:12:33  6 Feb 2020
Size is 287713 bytes
Description: None

2) user-checkpoint-1:
Created at 16:54:18 15 Sep 2020
Size is 7647 bytes
Description: None

3) user-checkpoint-2:
Created at 16:54:49 15 Sep 2020
Size is 7647 bytes
```

Table 1-3 Output Fields of the show checkpoint summary Command

Field	Description

Field	Description
user-checkpoint-1	Checkpoint name.
Created at 16:08:30 30 May 2014	Checkpoint creation time.
Size is 3,566 bytes	Size of the checkpoint configurations.
Description: None	Checkpoint description. This example indicates that no description is provided.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.54 show clock

Function

Run the **show clock** command to display the software time of the system.

Syntax

show clock

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the software time of the system.

```
Hostname> enable
Hostname# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

Table 1-4 Output Fields of the show clock Command

Field	Description
18:22:20	Hours, minutes, and seconds
UTC	Time zone
Tue	Week
Dec 11	Month and day
2012	Year

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 show cpu

Function

Run the **show cpu** command to display CPU usage information of system tasks on control cores and non-virtual cores.

Syntax

show cpu [**core**]

Parameter Description

core: Displays CPU usage information of each core on all boards.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

- This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.
- If the system is equipped with a virtual core, you can run the **show processes cpu** command to display the CPU usage of the virtual core.

Examples

The following example displays CPU usage of system tasks on control cores and non-virtual cores.

```
Hostname> enable
Hostname# show cpu
================================================
CPU Using Rate Information
CPU utilization in five seconds:  4.80%
CPU utilization in one minute:  4.10%
CPU utilization in five minutes:  4.00%
NO     5Sec    1Min    5Min Process
    1   0.00%   0.00%   0.00% init
    2   0.00%   0.00%   0.00% kthreadd
    3   0.00%   0.00%   0.00% ksoftirqd/0
    4   0.00%   0.00%   0.00% events/0
--More--
```

Table 1-5 Output Fields of the show cpu Command

Field	Description
CPU utilization in five seconds	Average CPU usage in five seconds
CPU utilization in one minute	Average CPU usage in one minute
CPU utilization in five minutes	Average CPU usage in five minutes
NO	No.
5Sec	Average CPU usage in five seconds
1Min	Average CPU usage in one minute
5Min	Average CPU usage in five minutes
Process	Process name

The following example displays the CPU usage information of each core on all boards.

```
Hostname> enable
Hostname# show cpu core
================================================
[Slot 2: M18000-16XS-CB, Cpu 0]
Core   5Sec   1Min   5Min
   0  11.9%  11.7%  23.4%
   1   0.0%   0.0%   0.0%
================================================
[Slot 3: M18000-16XS-CB, Cpu 0]
Core   5Sec   1Min   5Min
   0  11.2%  11.4%  23.7%
```

```
  1   0.0%   0.0%   0.0%
================================================
[Slot M1: M7800E-CM]
Core   5Sec   1Min   5Min
   0  15.9%  21.0%  29.7%
   1   1.5%   1.5%   1.4%
```

Table 1-6 Output Fields of the show cpu core Command

Field	Description
Slot	ID of the board slot
Cpu	ID of the board CPU slot
Core	Core ID
5Sec	Average CPU usage in five seconds
1Min	Average CPU usage in one minute
5Min	Average CPU usage in five minutes

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 show debugging

Function

Run the **show debugging** command to check whether the debugging function of the device is enabled.

Syntax

show debugging

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example checks whether the debugging function of the device is enabled.

```
Hostname> enable
Hostname# show debugging
mstp ha debug:
mstp ha debugging is on
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.57 show hostname

Function

Run the **show hostname** command to display the host name of the device.

Syntax

show hostname

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the host name of the device.

```
Hostname> enable
Hostname# show hostname
Hostname
Hostname#
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.58 show language character-set

Function

Run the **show language character-set** command to display the character set encoding format of the device.

Syntax

show language character-set

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the character set encoding format of the device.

```
Hostname> enable
Hostname# show language character-set
Current language character set encode: UTF-8
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.59 show line

Function

Run the **show line** command to display configurations of a line.

Syntax

show line { **console** *console-line-number* | **vty** *vty-line-number* | *line-number* }

Parameter Description

console *console-line-number*: Displays configurations of the console line. *console-line-number* indicates the console line ID. The value is **0**.

vty *vty-line-number*: Displays configurations of a virtual terminal line. *vty-line-number* indicates the virtual terminal line ID. The range is from 0 to 35.

line-number: ID of the specified line . The range is from 0 to 5.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays configurations of the console line.

```
Hostname> enable
Hostname# show line console 0
CON    Type    speed   Overruns
* 0    CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
            ^^x    none       ^M
Timeouts:     Idle EXEC    Idle Session
            never       never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output:  395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

Table 1-7 Output Fields of the show line Command

Field	Description
CON	Terminal type. **CON** indicates the console. **0** indicates the terminal line ID. The ID with an asterisk (*) indicates the terminal line that is being used.
Type	Terminal type, including **CON**, **AUX**, **TTY**, and **VTY**.
speed	Asynchronous speed
Overruns	Count of overrun errors received by the driver
Line 0	Terminal line ID
Location: ""	Line location
Type: "vt100"	Compatible terminal standard of a line
Special Chars	Special characters of a terminal, including the **Escape**, **Disconnect**, and **Activation** characters
Timeouts	Timeout time of a terminal session. **never** indicates that a session never times out.
History	Historical command recording function and the maximum number of recorded historical commands.
Total input	Count of data received from the driver
Total output	Count of data sent to the driver
Data overflow	Count of received data that overflows
stop rx interrupt	Count of RX interrupts of the driver

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.60 show memory

Function

Run the **show memory** command to display memory information.

Syntax

show memory [**history** | **low-watermark** | *process-id* | *process-name* | **slot** | **sorted total**]

Parameter Description

history: Displays historical memory usage records.

low-watermark: Displays the memory usage lower threshold.

process-id: Task ID.

process-name: Task name.

slot: Displays the memory usage information of all in-service devices in the system (without process usage information).

sorted total: Sorts tasks based on the memory usage.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

Each time the **show memory history** command is run, the number of displayed entries increases by one. Up to 10 entries are displayed. You can run the **memory history clear** command to clear historical entries.

Examples

The following example displays the memory usage of each task and its ranking by total memory usage.

```
Hostname> enable
Hostname# show memory sorted total
System Memory: 508324K total, 481560K used, 26764K free, 348200K available, 50.5% used
rate
Swap:        128000K total, 128000K free
Used detail:  149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K
others
PID    Text(K) Rss(K)  Data(K)        Stack(K) Total(K)       Process
807    1568    4584    264728         84       270028         tcpip.elf
854    40      1436    246076         84       248840         cli-filesystem
1237   52      1492    123260         84       126036         cli-memory
803    56      1104    74064          84       76920          ping.elf
727    84      1276    33812          84       36640          rg_syslogd
733    84      796     33536          84       36364          rg_syslogd
776    224     1416    16896          84       19800          lsmdemo
858    40      1324    16844          84       19612          rg-tty-admin
769    40      3600    11052          84       13812          skbdemo
--More--
```

Table 1-8 Description of Keywords in the Output of the show memory sorted total Command

Field	Description
total	Total memory size of the system

Field	Description
used	Size of the used memory
free	Size of the remaining memory
available	Size of the remaining available memory, including the idle memory size and idle swap area size
used rate	Memory usage in percentage For devices that use a swap area, the memory usage includes the swap area usage.
Swap	Total size and idle size of the swap area
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by the slab
others	Size of the used memory excluding the memory occupied by active and inactive pages, mapped memory, and slab memory.

Table 1-9 Output Fields of the show memory sorted Command

Field	Description
PID	Process ID
Text	Code segment size
Rss	Resident memory size
Data	Data segment size
Stack	Stack size
Total	Total used memory
Process	Task name

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **memory history clear**

1.61 show memory vsd

Function

Run the **show memory vsd** command to display memory information.

Syntax

show memory vsd *vsd_id*

Parameter Description

vsd_id: ID of the specified VSD. The range is from 0 to 16.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

You can run the **show vsd** command to display the ID of each VSD.

Examples

The following example displays the memory usage of tasks under VSD 1.

```
Hostname> enable
Hostname# show memory vsd 1
PID    Text    Rss    Data    Stack   Total   Process
1408   244     1192   25400   84      32164   tty_secu_enable
1385   104     16288  648     84      18648   gvpd
1384   304     3872   17084   84      24728   wbamain
1382   376     17708  33656   84      53308   snooping.elf
1381   84      2156   16736   84      22956   password_policy
1380   72      1096   404     84      3848    dns_client.elf
1379   168     2580   472     84      5352    rg-rmond
1378   652     3504   9768    84      15964   rg-snmpd
1376   208     1452   10672   84      14872   rg-fsui
1375   116     2020   33464   84      37288   rg-telnetc
1373   24      844    220     84      2824    rg-telnetd
1372   724     2364   17016   84      24380   rg-sshd
1371   244     2996   35780   84      42544   rg-tty-admin
1365   132     2168   9004    84      13796   vrrp_plus.elf
1364   312     16944  764     84      20368   vrrp.elf
1363   124     16988  500     84      19744   lacp.elf
```

```
1358    24      1380    320     84      3536    ftpc_cli.elf
1357    124     1944    8552    84      14976   ftp_server.elf
1352    340     3032    74704   84      80768   dhcp6.elf
1351    312     1960    988     84      6116    dhcp.elf
1350    388     17808   920     84      21600   mstp.elf
1349    240     3876    976     84      9536    rpi.elf
1348    1316    4656    1004    84      10764   isis.elf
1347    212     4220    872     84      9368    ripng.elf
1345    460     4284    876     84      9656    rip.elf
1344    1800    5568    1572    84      12156   bgp.elf
1340    1084    4700    1024    84      10928   ldp.elf
1339    288     17684   556     84      21472   msf.elf
1338    208     3604    42712   84      47708   rg-syslogd
--More--
```

Table 1-10 Output Fields of the show memory vsd Command

Field	Description
PID	Process ID
Text	Code segment size
Rss	Resident memory size
Data	Data segment size
Stack	Stack size
Total	Total used memory
Process	Task name

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 show pci-bus

Function

Run the **show pci-bus** command to display information about devices mounted on the Peripheral Component Interconnect (PCI) bus.

Syntax

show pci-bus

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about devices mounted on the PCI bus.

```
Hostname> enable
Hostname# show pci-bus
NO:0
Vendor ID           : 0x1131
Device ID           : 0x1561
Domain:bus:dev.func   : 0000:00:05.0
Status / Command     : 0x2100000
Class / Revision     : 0xc031030
Latency            : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a
NO:1
Vendor ID           : 0x1131
Device ID           : 0x1562
Domain:bus:dev.func   : 0000:00:05.1
Status / Command     : 0x2100156
Class / Revision     : 0xc032030
Latency            : 0x30
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
```

```
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 show processes cpu

Function

Run the **show processes cpu** command to display system tasks.

Syntax

show processes cpu [**history** [**table**] | [**5sec** | **1min** | **5min** | **15min**] [**nonzero**]]

Parameter Description

history: Displays the CPU usage of control core tasks within the last 60 seconds, 60 minutes, and 72 hours in histogram.

table: Displays the CPU usage of control core tasks within the last 60 seconds, 60 minutes, and 72 hours in table.

5sec: Displays tasks in descending order of the CPU usage within the last 5 seconds.

1min: Displays tasks in descending order of the CPU usage within the last 1 minute.

5min: Displays tasks in descending order of the CPU usage within the last 5 minutes.

15min: Displays tasks in descending order of the CPU usage within the last 15 minutes.

nonzero: Not displays information about the tasks whose CPU usage is 0.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

Examples

The following example displays tasks in ascending order of their IDs.

```
Hostname> enable
Hostname# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)
Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S   PRI  P      5Sec      1Min      5Min     15Min Process
    1   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) init
    2   0 S    20  1   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) kthreadd
    3   0 S  -100  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) migration/0
    4   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) ksoftirqd/0
    5   0 S  -100  1   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) migration/1
--More--
```

Table 1-11 Output Fields of the show processes cpu Command

Field	Description
System Uptime	Total running time of the device, accurate to seconds
CPU Utilization	Total CPU usage of control core tasks within the last 5 seconds, 1 minute, and 5 minutes
Virtual CPU usage	Total CPU usage of virtual core tasks within the last 5 seconds, 1 minute, and 5 minutes
Tasks Statistics	Task statistics, including the total number of tasks and the task status
set system cpu watermark	CPU usage threshold and status of the control core tasks

Table 1-12 Description of the Task Running Status in the Output of the show processes cpu Command

Task Running Status	Description
running	Running task
sleeping	Suspended task
stopped	Stopped task
zombie	Terminated task, but not reclaimed by the system

Table 1-13 Description of Task Information in the Output of the show processes cpu Command

Field	Description

Field	Description
Pid	Task ID
Vsd	VSD ID
S	Task statuses, including **R** (running), **T** (stopped), **S** (sleeping), **D** (waiting), and **Z** (zombie)
PRI	Task priority
P	CPU core on which a task runs
5sec/1min/5min/15min	CPU usage of a task within the last 5 seconds, 1 minute, 5 minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores of the same type as the core where the task runs.
Process	Task name. Only the first 15 characters are displayed. The remaining characters are truncated.

The following example displays the CPU usage of a control core task within the last 60 seconds, 60 minutes, and 72 hours in histogram.

```
Hostname> enable
Hostname# show processes cpu history
           system cpu percent usage(%) [last 300 second]

    —
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|*********
   35|||||||||||
   30|||||||||||*
   25||||||||||||
   20||||||||||||
   15||||||||||||
   10||||||||||||
    5||||||||||||***************
    0|||||||||||||||||||||||||||
```

```
    #=========#=========#=====*==>
    0        50       100     second
        system cpu percent usage(%) per 5second (last 125 second)
--------------------------------------------------------------------------------
            system cpu percent usage(%) [last 60 minute]

    _
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|
   35|
   30|*
   25||
   20||
   15||
   10||
    5||*
    0|||
     #==*==>
     0    minute
        system cpu percent usage(%) per 1minute (last 2 minute)
--------------------------------------------------------------------------------
```

In the preceding output information:

The first histogram displays the CPU usage of the control core tasks within 300 seconds. Each segment on the x-coordinate indicates 5 seconds, and each segment on the y-coordinate indicates 5%. "*" indicates the CPU usage at the moment of a second. The first segment nearest to 0 on the x-coordinate indicates the CPU usage within the last 5 seconds, in percentage (%).

The second histogram displays the CPU usage of the control core tasks within the last 60 minutes, in percentage (%). Every segment on the x-coordinate indicates 1 minute.

The third histogram displays the CPU usage of the control core tasks within the last 72 hours, in percentage (%). Every segment on the x-coordinate indicates 1 hour.

The following example displays the CPU usage of tasks on core 0 within the last 60 seconds, 60 minutes, and 72 hours in table.

```
Hostname> enable
Hostname # show processes cpu history table
```

```
            system cpu percent usage(%) [last 300 second]
#-------------------------#
|     |   1|   2|   3|   4|   5|   6|   7|   8|   9|  10|
#-------------------------#
#-------------------------#
|     0| 2.0| 2.4| 2.3| 2.3| 2.8| 3.0| 2.7| 3.2| 2.6| 2.4|
#-------------------------#
|     1| 2.7| 2.5| 2.7| 2.2| 2.4| 2.6| 2.2| 2.7| 2.3| 2.5|
#-------------------------#
|     2| 2.9| 2.0| 2.4| 2.5| 2.7| 2.4| 2.4| 2.6| 2.6| 2.5|
#-------------------------#
|     3| 2.7| 2.8| 2.8| 3.2| 2.5| 3.2| 3.1| 4.0| 2.7| 2.7|
#-------------------------#
|     4| 4.0| 2.3| 2.1| 2.2| 2.7| 2.4| 2.5| 2.6| 2.4| 2.6|
#-------------------------#
|     5| 2.4| 3.2| 2.5| 2.3| 2.3| 3.6| 2.8| 2.5| 2.2| 2.4|
#-------------------------#
            system cpu percent usage(%) [last 60 minute]
#-------------------------#
|     |   1|   2|   3|   4|   5|   6|   7|   8|   9|  10|
#-------------------------#
#-------------------------#
|     0| 2.6| 2.5| 3.0| 2.4| 2.6|
#-------------------------#
```

In the preceding output information:

The first table lists the CPU usage within 300 seconds. The first segment indicates the CPU usage within the last 5 seconds, in percentage (%). Each segment indicates 5 seconds.

The second table lists the CPU usage within the last 60 minutes, in percentage (%). Each segment indicates 1 minute.

The third table lists the CPU usage within the last 72 hours, in percentage (%). Each segment indicates 1 hour.

The following example displays the CPU usage of control core tasks every 5 minutes in the last week that exceeds the CPU usage threshold.

```
Hostname> enable
Hostname# show processes cpu record
CPU watermark high up 9%, down 6%
1970-01-07 01:20:13    system(11.0%)   ssa_process(9.1%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  rl-con/0(0.2%)
 1970-01-07 01:25:26    system(10.8%)   ssa_process(9.1%)  ssd_process(0.6%)
ham(0.3%)  ssc_process(0.3%)  lsm.elf(0.2%)
 1970-01-07 01:30:39    system(10.5%)   ssa_process(9.0%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  rg-sysmon(0.2%)
 1970-01-07 01:35:52    system(10.5%)   ssa_process(9.0%)  ssd_process(0.6%)
ham(0.3%)  ssc_process(0.3%)  rg-sysmon(0.2%)
```

```
 1970-01-07 01:41:05    system(10.7%)   ssa_process(9.1%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  lsm.elf(0.2%)
 1970-01-07 01:46:18    system(10.7%)   ssa_process(9.1%)  ssd_process(0.6%)
ham(0.3%)  ssc_process(0.3%)  rg-sysmon(0.2%)
 1970-01-07 01:51:31    system(10.8%)   ssa_process(9.1%)  ssd_process(0.6%)
rg-sysmon(0.3%)  ssc_process(0.3%)  ham(0.3%)
 1970-01-07 01:56:45    system(10.9%)   ssa_process(9.1%)  ssd_process(0.6%)
ham(0.3%)  ssc_process(0.3%)  rg-sysmon(0.3%)
 1970-01-07 02:01:58    system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)
rg-sysmon(0.4%)  ssc_process(0.3%)  ham(0.3%)
 1970-01-07 02:07:11    system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)
rg-sysmon(0.4%)  ham(0.3%)  ssc_process(0.3%)
 1970-01-07 02:12:24    system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)
rg-sysmon(0.4%)  ssc_process(0.3%)  ham(0.3%)
 1970-01-07 02:17:37    system(11.0%)   ssa_process(9.0%)  ssd_process(0.6%)
rg-sysmon(0.4%)  ham(0.3%)  ssc_process(0.3%)
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 show processes cpu detailed

Function

Run the **show processes cpu detailed** command to display details about a specific task.

Syntax

show processes cpu detailed { *process-id* | *process*-name }

Parameter Description

process-id: ID of a specified task.

process-name: Name of a specified task.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

Examples

The following example displays details about a task with the specified name.

```
Hostname> enable
Hostname# show processes cpu detailed demo
Process Id    : 1820
Process Name  : demo
Vsdid        : 0
Process Ppid  : 1
State        : R(running)
On CPU       : 0
Priority     : 20
Age Time     : 24:06.5
Run Time     : 00:01.0
Cpu Usage    :
   Last  5 sec    0.3%(0.6%)
   Last  1 min    0.3%(0.6%)
   Last  5 min    0.3%(0.6%)
   Last 15 min    0.3%(0.6%)
Tty          : ?
Code Usage    : 209.6KB.
```

If the specified task name is not unique, the system displays the following information:

```
Hostname> enable
Hostname# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
name: demo, id: 1091, state: R(running)
process name: monitor_procps, do NOT exist, or NOT only one.
```

The following example displays details about a task with the specified ID.

```
Hostname> enable
Hostname# show process cpu detailed 1715
Process Id    : 130
Process Name  : crypto
Vsdid        : 0
Process Ppid  : 2
State        : S(sleeping)
On CPU       : 0
Priority     : 0
Age Time     : 03:41:09.9
Run Time     : 00:00.0
Cpu Usage    :
   Last  5 sec    0.0%(  0.0%)
```

```
   Last  1 min    0.0%(  0.0%)
   Last  5 min    0.0%(  0.0%)
   Last 15 min    0.0%(  0.0%)
Tty          : ?
Code Usage    : 0.0KB.
```

Table 1-14 Output Fields of the show processes cpu detailed Command

Field	Description
Process Id	Task ID
Vsdid	ID of the VSD to which the task belongs
Process Name	Task name
Process Ppid	Parent process task ID
State	Task running status
On CPU	CPU where the task is running
Priority	Task priority
Age Time	Duration of the task from startup to now
Run Time	Execution duration of the task from startup to now
Cpu Usage	CPU usage of the task within the last 5 seconds, 1 minute, 5 minutes, and 15 minutes The value in the round brackets is the CPU usage that is not divided by the total number of cores of the same type as the core where the task runs. For example, the demo task is running on core 0, which is a control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%).
Tty	TTY ID, in the format of "Master device ID, slave device ID". If the TTY ID is **0**, a question mark (?) is displayed.
Code Usage	Size occupied by the task code segment

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.65 show reload

Function

Run the **show reload** command to display system restart configuration.

Syntax

show reload

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays system restart configuration.

```
Hostname> enable
Hostname# show reload
System reload state: Warm
```

Table 1-15 Output Fields of the show reload Command

Field	Description
System reload state	System restart status

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.66 show running-config

Function

Run the **show running-config** command to display the running configurations of the device system or configurations of an interface.

Syntax

show running-config [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and ID.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays configurations of interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show running-config interface gigabitethernet 0/1

Building configuration...
Current configuration: 31 bytes

interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.67 show service

Function

Run the **show service** command to display the service status (enabled/disabled).

Syntax

show service

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the service status (enabled/disabled).

```
Hostname> enable
Hostname# show service
web-server   : disabled
web-server(https): disabled
snmp-agent   : enabled
ssh-server   : enabled
telnet-server : disabled
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.68 show sessions

Function

Run the **show sessions** command to display information about connected telnet clients.

Syntax

show sessions

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about connected telnet clients.

```
Hostname> enable
Hostname# show sessions
Conn  Address
*1    127.0.0.1
*2    192.168.21.122
```

Table 1-16 Output Fields of the show sessions Command

Field	Description
Conn	ID of a connected telnet client
Address	IP address of the connected telnet client

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.69 show startup-config

Function

Run the **show startup-config** command to display device configurations stored in the non-volatile random-access memory (NVRAM).

Syntax

show startup-config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The configurations stored in the NVRAM, namely, startup-config, are executed during device startup.

startup-config indicates configurations in the default configuration file **/config.text** embedded in the flash memory of the device by default.

Examples

The following example displays device configurations stored in the NVRAM.

```
Hostname> enable
version CS86_RGOS 12.6(2)B0103, Release(10151616)
hostname Hostname
!
vlan 1
 max-dynamic-mac-count 32767
!
vlan 2
 remote-span
!
vlan range 10,12,30,4094
!
sysmac 8005.883f.d00a
!
redundancy
 --More--
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.70 show sysmon grpc info

Function

Run the **show sysmon grpc info** command to display information about the gRPC function registered in the system monitoring process.

Syntax

show sysmon grpc info

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about the gRPC function registered in the system monitoring process of the device.

```
Hostname> enable
Hostname#show sysmon grpc info
% Sysmon grpc init state    : Success
% Sysmon grpc subscribe state: False
```

Table 1-17 Output Fields of the show sysmon grpc info Command

Field	Description
Sysmon grpc init state	Initialization status of the Sysmon service process
Sysmon grpc subscribe state	gRPC subscription status of the Sysmon service process

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.71 show telnet ip-block

Function

Run the **show telnet ip-block** command to display information about blocked IP addresses and authentication failures.

Syntax

show telnet ip-block { **all** | **list** }

Parameter Description

all: Displays information about all blocked IP addresses and authentication failures.

list: Displays information about blocked IP addresses.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about all blocked IP addresses and authentication failures, including the source IPv4 or IPv6 addresses, IP address status, and number of authentication failures

or IP address blocking information, including the source IPv4 or IPv6 addresses and remaining time for awakening the blocked IP addresses.

Examples

The following example displays information about all blocked IP addresses and authentication failures.

```
Hostname> enable
Hostname# show telnet ip-block all
-------------------------------------------------------------------------
IP Address                                State      Auth-fail Count
-------------------------------------------------------------------------
172.30.31.16                               AUTH FAILED    3
172.30.31.17                               BLOCKED        6
-------------------------------------------------------------------------
```

Table 1-18 Output Fields of the show telnet ip-block all Command

Field	Description
IP Address	Source IPv4 or IPv6 address
State	Status • **AUTH FAILED**: Authentication fails but the blocking conditions are not met. • **BLOCKED**: Blocking conditions are met.
Auth-fail Count	Number of authentication failures

The following example displays information about blocked IP address.

```
Hostname> enable
Hostname# show telnet ip-block list
-------------------------------------------------------------------------
IP Address                                UnBlock Interval (Seconds)
-------------------------------------------------------------------------
172.30.31.17                               296
-------------------------------------------------------------------------
```

Table 1-19 Output Fields of the show telnet ip-block list Command

Field	Description
IP Address	Source IPv4 or IPv6 address
UnBlock Interval (Seconds)	Remaining time for awakening blocked IP addresses, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.72 show this

Function

Run the **show this** command to display effective system configurations in current mode.

Syntax

show this

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

In range mode, this command can be used to display configurations in current mode. For example, after you perform the following operations, you can run this command to display effective configurations in the current mode.

- Run the **line** *first-line last-line* command to specify a line scope and enter the line configuration mode.
- Run the **vlan range** command to configure multiple Virtual Local Area Networks (VLANs) and enter the VLAN range configuration mode.
- Run the **vlan range** command to configure multiple interfaces and enter the interface range configuration mode.

> **Note**
>
> If the number of VLANs or interfaces exceeds 50 in VLAN range configuration mode or interface range configuration mode, this command only displays configurations of the first 50 VLANs or interfaces.

Examples

The following example displays effective configurations of GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-gigabitethernet 0/1)# show this
Building configuration...
 !
 spanning-tree link-type point-to-point
 spanning-tree mst 0 port-priority 0
 !
end
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.73 show usb-bus

Function

Run the **show usb-bus** command to display information about devices mounted on the USB bus.

Syntax

show usb-bus

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about devices mounted on the USB bus.

```
Hostname> enable
Hostname# show usb-bus
Device: Linux Foundation 2.0 root hub
  Bus 001 Device 001: ID 1d6b:0002
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.74 show version

Function

Run the **show version** command to display the system version.

Syntax

show version

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the system version.

```
Hostname> enable
Hostname# show version
System description     : Ruijie 10G Ethernet Switch(CS86-48MG4VS2QXS-UPD) By Ruijie
Networks
System start time      : 2023-03-20 11:53:50
```

```
System uptime          : 00:00:05:44
System hardware version : 1.00
System software version : CS86_RGOS 12.6(2)B0103, Release(10151616)
System patch number    : NA
System software number  : M16542103162023
System serial number    : 1234942570042
System boot version     : 1.4.27(Master) 1.4.20(Slave)
System rboot version    : 1.1.39
System core version     : 4.4.178-g45e9d32-dirty
Module information:
  Slot 1/0 : CS86-48MG4VS2QXS-UPD
    System uptime       : 00:00:05:29
    Hardware version    : 1.00
    Boot version        : 1.4.27(Master) 1.4.20(Slave)
    Rboot version       : 1.1.39
    Software version    : CS86_RGOS 12.6(2)B0103, Release(10151616)
    Software number     : M16542103162023
    Serial number       : 1234942570042
  Slot 2/0 : CS86-24MG4VS-UP
    System uptime       : 00:00:05:44
    Hardware version    : 1.00
    Boot version        : 1.4.27(Master) 1.4.21(Slave)
    Rboot version       : 1.1.39
    Software version    : CS86_RGOS 12.6(2)B0103, Release(10151616)
    Software number     : M16542103162023
    Serial number       : 1234942570039
```

Table 1-20 Description of Keywords in the Output of the show version Command

Field	Description
System description	Product description
System starttime	System startup time
System uptime	System running time
System hardware version	System hardware version
System software version	System software version
System patch number	System patch version number
System serial number	Product SN
System boot version	System boot version
System rboot version	System rboot version
Module information	System module information

Table 1-21 Description of Module Information in the Output of the show version Command

Field	Description
Slot	Slot ID
System uptime	Running time of the board
Hardware version	Hardware version of the board
Boot version	Boot version of the board
Rboot version	Reboot version of the board
Software version	Software version of the board
Serial number	SN of the board

Notifications

- System start time: Indicates the startup time of cluster devices. The time is not reset before all management devices in the cluster are restarted at the same time.
- System uptime: Indicates the cluster running time. The time is not reset before all management devices in the cluster are restarted at the same time.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.75 telnet

Function

Run the **telnet** command to log in to the telnet server.

Syntax

telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

Parameter Description

oob: Connects to a remote telnet server through out-of-band communication (over the MGMT port typically).

hostname: Host name of the telnet server.

ipv4-address: IPv4 host address of the telnet server.

ipv6-address: IPv6 host address of the telnet server.

port-number: TCP port number of the telnet server. The range is from 0 to 65535, and the default value is **23**.

/source: Specifies the source IP address or source interface used by the telnet client.

ip *ipv4-address*: Specifies the source IPv4 address used by the telnet client. *ipv4-address* indicates an IPv4 address.

ipv6 *ipv6-address*: Specifies the source IPv6 address used by the telnet client. *ipv6-address* indicates an IPv6 address.

interface *interface-type interface-name*: Specifies the source interface used by the telnet client. *interface-type interface-name* indicates the specified interface type and ID.

via *mgmt-name*: Specifies the MGMT port used by the telnet client for the **oob** parameter. *mgmt-name* indicates the MGMT port number.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example sets the IPv4 address of the telnet server to **192.168.1.1**, the TCP port number to the default value, the source interface to **Gi 0/1**, and the VRF table to **vpn1**.

```
Hostname> enable
Hostname# telnet 192.168.1.1 /source interface gigabitethernet 0/1 /vrf vpn1
```

The following example sets the IPv6 address of the telnet server to **2AAA:BBBB::CCCC**.

```
Hostname> enable
Hostname# telnet 2AAA:BBBB::CCCC
```

The following example sets the IPv4 address of the telnet server to **192.168.1.1** and uses MGMT 0 for the **oob** parameter.

```
Hostname> enable
Hostname# telnet oob 192.168.1.1 via mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.76 username

Function

Run the **username** command to configure a local user account and optional authorization information.

Run the **no** form of this command to remove this configuration.

No local user account or authorization information is configured by default.

Syntax

username *username* [**login mode** { **console** | **ssh** | **telnet** | **ftp** }] [**online amount** *amount-number*] [**permission** *oper-mode path*] { [**privilege** *privilege-level*] | [**role** *text-string*] } [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string* | **secret** [**0** | **5** | **8**] *text-string*]

no username *name*

Parameter Description

username: Account username.

login mode { **console** | **ssh** | **telnet** | **ftp** }: Restricts the account login method. **console** indicates that the account login method is restricted to console. **ssh** indicates that the account login method is restricted to SSH. **telnet** indicates that the account login method is restricted to telnet. **ftp** indicates that the account login method is restricted to FTP.

online amount *amount-number*: Configures the number of concurrently online accounts. *amount-number* indicates the number of concurrently online accounts. The range is from 0 to 1586. The default value is **0**, that is, the number of concurrently online accounts is not limited.

permission *oper-mode path*: Configures the operation permission of an account on a specific file. *oper-mode* indicates the operation mode. **n** indicates no operation behavior. **r** indicates the read permission. **w** indicates the write permission. **x** indicates the execution permission. **rw** indicates the read and write permissions. **rx** indicates the read and execution permissions. **wx** indicates the write and execution permissions. **rwx** indicates the read, write, and execution permissions. *path* indicates the path of the file or directory, on which an operation permission takes effect.

privilege *privilege-level*: Configures the privilege level of an account. *privilege-level* indicates the privilege level of an account. The range is from 0 to 15.

reject remote-login: Bans remote login.

web-auth: Allows only Web authentication.

pwd-modify: Allows the Web authentication user who uses this account to change the password. This parameter is available only after **web-auth** is configured.

nopassword: Configures no password for the account.

password [**0** | **7**] *text-string*: Configures a simple password for the account. **0** indicates that a plaintext password is entered. **7** indicates that a ciphertext password is entered. No plaintext password is entered by default. *text-string* indicates the password text.

secret [**0** | **5** | **8**] *text-string*: Configures a secure password for the account. The password configured by this command is stored as a ciphertext password after irreversible encryption. **0** indicates that a plaintext password is entered, **5** indicates that a password encrypted using the MD5 algorithm is entered, **8** indicates that a password encrypted using the SHA-256 algorithm is entered. A plaintext password is entered by default.

role *text-string*: Adds roles to the local user when the RBAC mode is enabled. A maximum of 64 roles can be added.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- This command is used to create a local user database for authentication.
- The encryption type **7** is specified only when encrypted passwords are copied and pasted.
- If the value **7** is specified as the encryption type, the entered ciphertext string must consist of an even number of characters.

Examples

The following example configures a username and password and binds the account to privilege level 15.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# username test privilege 15 password 0 pw15
```

The following example configures a dedicated username and password for Web authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# username user1 web-auth password 0 pw
```

The following example configures user **test** to have the permissions to read and write all files and directories.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# username test permission rw /
```

The following example configures user **test** to have the permissions to read, write, and execute all files and directories except the **config.text** file.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# username test permission n /config.text
Hostname(config)# username test permission rwx /
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.77 username export

Function

Run the **username export** command to export user information to a text file.

Syntax

username export *filename*

Parameter Description

filename: Name of the file used to save exported user information.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example exports user information to the **user.csv** file.

```
Hostname> enable
Hostname# username export user.csv
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.78 username import

Function

Run the **username import** command to import user information from a text file.

Syntax

username import *filename*

Parameter Description

filename: Name of the file to be imported.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example imports user information from the **user.csv** file.

```
Hostname> enable
Hostname# username import user.csv
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.79 write

Function

Run the **write** command to save system configurations (running-config) to a specific position.

Syntax

write [**auto-save interval** *interval-time* | **memory** [**auto-save interval** *interval-time*] | **terminal**]

Parameter Description

auto-save interval *interval-time*: Sets the interval for automatic saving in seconds. The range is from 600 to 86400. The default value is **3600**.

memory: Writes system configurations to the NVRAM. It is equivalent to the **copy running-config startup-config** command.

terminal: Displays system configurations. It is equivalent to the **show running-config** command.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If there is a device to save the configuration file, the system automatically creates a specified file and writes system configurations to the file.

In the absence of such a device, for example, as the startup configuration file is specified to be in a portable storage device, such as a USB flash drive or SD card but the device is not loaded during the execution of the **write** [**memory**] command, the system asks you whether to save the current configurations to the default startup configuration file **config.text** and performs corresponding operations.

Examples

The following example saves system configurations to the device.

```
Hostname> enable
Hostname# write
Building configuration...
[OK]
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 RBAC Commands

Command	Function
description	Configure the description of a role.
feature	Add a feature to a feature group.
interface policy deny	Prohibit a role from operating all interface resources.
permit interface	Allow a role to operate a specific interface resource.
permit vlan	Allow a role to operate a specific VLAN resource.
permit vrf	Allow a role to operate a specific VRF resource.
role enable	Enable the RBAC function.
role feature-group name	Configure a feature group and enter the specified feature group configuration mode.
role name	Configure a role and enter a specified role configuration mode.
rule	Configure rule permissions for a role.
show role	Show information about a specific role or all roles.
show role feature	Display the basic information or details about a specific feature or all features.
show role feature-group	Display the basic information or details about a specific feature group or all feature groups.
vlan policy deny	Prohibit a role from operating all VLAN resources on a device.
vrf policy deny	Prohibit a role from operating all VRF resources.

1.1 description

Function

Run the **description** command to configure the description of a role.

Run the **no** form of this command to restore the default description of a role.

Run the **default** form of this command to restore the default configuration.

By default, a predefined role is provided with a default description while a user-defined role is provided with no description.

Syntax

description *description*

no description

default description

Parameter Description

description: Description of a role. It is a string of 1 to 128 characters.

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to configure the description of a role.

Examples

The following example configures description "admin role" for role **admin-role**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# description admin role
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**

- role name
- show role

1.2 feature

Function

Run the **feature** command to add a feature to a feature group.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

By default, a predefined feature group contains default features while a user-defined feature group contains no feature.

Syntax

feature *feature-name*

no feature *feature-name*

default feature *feature-name*

Parameter Description

feature-name: The feature to be added to a specified feature group. *feature-name* indicates the name of a feature predefined in the system and is case-sensitive.

Command Modes

Feature group configuration mode

Default Level

15

Usage Guidelines

This command is used to add a feature to a feature group.

Examples

The following example adds feature **aaa** to feature group **test-group**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role feature-group name test-group
Hostname(config-role-featuregrp)# feature aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role feature-group name
- show role feature-group

1.3 interface policy deny

Function

Run the **interface policy deny** command to prohibit a role from operating all interface resources.

Run the **no** form of this command to allow a role to operate all interface resources .

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all interface resources.

Syntax

interface policy deny

no interface policy deny

default interface policy deny

Parameter Description

N/A

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all interface resources.

Examples

The following example prohibits the role **admin-role** from operating all interface resources.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role name
- show role

1.4 permit interface

Function

Run the **permit interface** command to allow a role to operate a specific interface resource.

Run the **no** form of this command to prohibit a role from operating a specific interface resource or all interface resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all interface resources.

Syntax

permit interface *interface-type interface-number-list*

no permit interface [*interface-type interface-number-list*]

default permit interface [*interface-type interface-number-list*]

Parameter Description

interface *interface-type interface-number-list*: Specifies the interface type and interface number list. An interface number list contains one or more interface numbers. Interface numbers are separated by a comma (,). You can specify an interface number range by connecting the first and the last interface numbers with a hyphen (-).

Command Modes

Role interface configuration mode

Default Level

15

Usage Guidelines

This command is used to allow a role to operate interface resources.

Examples

The following example allows role **admin-role** to operate GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
Hostname(config-role-interface)# permit interface gigabitethernet 0/1
```

The following example allows role **admin-role** to operate GigabitEthernet 0/2, GigabitEthernet 0/4, and GigabitEthernet 0/6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
Hostname(config-role-interface)# permit interface gigabitethernet 0/2, 0/4, 0/6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **interface policy deny**
- **show role**

1.5 permit vlan

Function

Run the **permit vlan** command to allow a role to operate a specific VLAN resource.

Run the **no** form of this command to prohibit a role from operating a specific VLAN resource or all VLAN resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all VLAN resources.

Syntax

permit vlan *vlan-list*

no permit vlan [*vlan-list*]

default permit vlan [*vlan-list*]

Parameter Description

vlan-list: VLAN list. The value range is from 1 to 4094. The VLAN list can contain one or more VLANs. VLAN IDs are separated by a comma (,). You can specify a VLAN range by connecting the first and the last VLAN IDs with a hyphen (-).

Command Modes

Role VLAN configuration mode

Default Level

15

Usage Guidelines

This command is used to allow a role to operate VLAN resources.

Examples

The following example allows the role **admin-role** to operate VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
Hostname(config-role-vlan)# permit vlan 1
```

The following example allows the role **admin-role** to operate VLAN 1, VLAN 3, and VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
Hostname(config-role-vlan)# permit vlan 1,3,5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **vlan policy deny**
- **show role**

1.6 permit vrf

Function

Run the **permit vrf** command to allow a role to operate a specific VRF resource.

Run the **no** form of this command to prohibit a role from operating a specific VRF resource or all VRF resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all VRF resources.

Syntax

permit vrf *vrf-name*

no permit vrf [*vrf-name*]

default permit vrf [*vrf-name*]

Parameter Description

vrf-name: VRF instance name.

Command Modes

Role VRF configuration mode

Default Level

15

Usage Guidelines

This command allows a role to operate VRF resources on a device.

Examples

The following example allows the role **admin-role** to operate VRF instance **test** .

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vrf policy deny
Hostname(config-role-vrf)# permit vrf test
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **vrf policy deny**
- **show role**

1.7 role enable

Function

Run the **role enable** command to enable the RBAC function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The RBAC function is disabled by default.

Syntax

role enable

no role enable

default role enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to enable or disable the RBAC function.

Examples

The following example enables the RBAC function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 role feature-group name

Function

Run the **role feature-group name** command to configure a feature group and enter the specified feature group configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, feature groups **L2** and **L3** are predefined in the system, and these feature groups contain features.

Syntax

role feature-group name *group-name*

no role feature-group name *group-name*

default role feature-group name *group-name*

Parameter Description

group-name: Name of a feature group. It is a case-sensitive string of 1 to 32 characters.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to create a feature group and enter the feature group configuration mode.

The system predefines feature groups **L2** and **L3**. **L2** contains all commands for functions related to L2 protocols, and **L3** contains all commands for functions related to L3 protocols. The predefined feature groups cannot be deleted or modified. Users can customize up to 64 feature groups and configure features for the feature groups.

Examples

The following example configures feature group **test-group** for a role, and enters the feature group configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role feature-group name test-group
Hostname(config-role-featuregrp)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **show role feature-group**

1.9 role name

Function

Run the **role name** command to configure a role and enter a specified role configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-***n* (0–15). Each role is granted with specific operation permissions.

Syntax

role name *role-name*

no role name *role-name*

default role name *role-name*

Parameter Description

role-name: Name of a role. It is a case-sensitive string of 1 to 64 characters.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to create a role and enter the role configuration mode.

The system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-***n* (0–15).

System predefined roles cannot be deleted by running the **no** command. The default permission of only the **priv-***n* (0–13) role can be restored by running the **default** command.

Permissions can be added to the **priv-***n* (0–13) role only. System predefined permissions cannot be deleted, and permissions of other roles cannot be modified.

Users can customize up to 64 roles and configure permissions for the roles.

Examples

The following example configures role **admin-role** and enters the role configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **show role**

1.10 rule

Function

Run the **rule** command to configure rule permissions for a role.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, predefined roles have predefined rule permissions while user-defined roles have no rule permissions.

Syntax

rule *rule-number* { **permit** | **deny** } { **command** *command-string* | { **read** | **write** | **execute** }* { **feature** [*feature-name*] | **feature-group** *feature-group-name* } }

no rule { *rule-number* | **all** }

default rule { *rule-number* | **all** }

Parameter Description

rule-number: Rule ID. The value range is from 1 to 256.

permit: Allows the user to execute the specified command.

Deny: Prohibits the user from executing the specified command.

command *command-string*: Configures command-based rules. *command-string* indicates a case-sensitive command string of 1 to 128 characters. It can be a specific command or multiple commands that are separated by a semicolon (;). It can also be a type of commands represented by an asterisk (*) wildcard. *command-string* can contain spaces and all printable characters.

read: Indicates a read command, that is, a type of commands that can display system configurations and maintenance information, such as the **show**, **dir**, and **more** commands.

write: Indicates a write command, that is, a type of commands that can configure the system, for example, the **logging on** command.

execute: Indicates an execution command, that is, a type of commands that can execute a specific program or function, for example, the **ping** command.

feature *feature-name*: Configures feature-based rules. *feature-name* indicates the name of a feature predefined in the system and is case-sensitive. If no feature name is specified, the command applies to all features.

feature-group *feature-group-name*: Configures feature group-based rules. *feature-group-name* indicates the name of a feature group. It is a case-sensitive string of 1 to 32 characters.

all: Specifies all permission rules.

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to configure rule permissions for a role. Note:

- During rule configuration, if the specified rule number does not exist, create a rule; otherwise, modify the rule corresponding to the rule number. The modified rule supports newly authenticated users only.
- A user role is allowed to create multiple rules, and permissions executable by this role is a union set of these rules. If permissions defined by these rules conflict with each other, rules with larger serial numbers prevail. For example, if command A is prohibited by rule 1, and command B is prohibited by rule 2, but command A is allowed by rule 3, rule 2 and rule 3 finally take effect. Specifically, command A is allowed and command B is prohibited.
- Predefined rules for predefined roles cannot be deleted or modified. If there is a conflict between system predefined rules and user-defined rules, user-defined rules prevail.
- Up to 256 rules can be configured for each role. A maximum of 1024 rules are configured for all roles on the device.

To configure command-based rules, follow the rules below:

- Division of segments
  - To describe a multi-level mode command, divide the command character string into multiple segments by a semicolon (;). Each segment represents one or a series of commands. The command in the latter segment is used to execute the mode of a command in the preceding segment.
  - A segment must contain at least one printable character.
- Use of semicolons
  - To describe a multi-level mode command, divide the command segments with a semicolon. For example, the character string **config ; logging on** is used to grant a permission over the **logging on** command in configuration mode.
  - The semicolon in the last command segment indicates that the permission is granted over the current mode command. For example, the character string **config ; interface *** grants a permission over only the command in interface configuration mode.
  - The absence of a semicolon in the last command segment indicates that permissions are granted over the current command mode and all commands in this mode. For example, the character string **config ; interface *** is used to grant permissions over all commands in interface mode.
- Use of asterisks
  - Each command segment can contain at least one asterisk (*). An asterisk resides either in the middle or at both ends of a command segment. Each asterisk serves to fuzzily match a command. For example, the character string **config ; *** is used to grant permissions over all commands in configuration mode. The character string **config ; logging * flush** is used to grant a permission over a command starting with **logging** and ending with **flush** in configuration mode. The character string **config ; logging *** is used to grant permissions over all the commands starting with **logging** in configuration mode.

- When an asterisk resides in the middle of a command segment and the asterisk is used to match the command, the command is matched up to only the first asterisk in the middle, and the subsequent command segments are all considered matched. An execution command must be fully matched.

- Matching of keyword prefixes
  - A prefix matching algorithm is used for the matching between the command keyword and the command character string. That is, if the first several consecutive characters or all characters of a keyword in the command line match the keyword defined in a rule, the command line matches this rule. Therefore, a command character string may include a partial or complete command keyword. For example, if the rule **rule 1 deny command show ssh** is effective, the **show ssh** and **show ssh-session** commands are disabled.

Examples

The following example configures role **admin-role**, which has rule permissions to run all commands in configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# rule 1 permit command config ; *
```

The following example configures role **admin-role**, which has the permission to read feature **aaa**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# rule 2 permit read feature aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **show role**

1.11 show role

Function

Run the **show role** command to show information about a specific role or all roles.

Syntax

show role [**name** *role-name*]

Parameter Description

name *role-name*: Displays information about a specific role.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about a specific role or all roles.

Examples

The following example displays information about the role **network-admin**.

```
Hostname> enable
Hostname# show role name network-admin
Role: network-admin
  Description: Predefined network admin role has access to all commands
  Interface policy: permit (default)
  VLAN policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ------------------------------------------------------------------
  sys-1   permit      command      *
  R:Read W:Write X:Execute
```

Table 1-1 Output Fields of the show role name Command

Field	Description
Role	Name of a role.
Description	Description of a role.
Interface policy	Allows a role to operate all interface resources.
VLAN policy	Allows a role to operate all VLAN resources.
Vrf policy	Allows a role to operate all VRF resources.
Rule	Rule ID.
Perm	Allow or prohibit.
Type	Command type. This field is set to **RWX**, indicating that the permissions to read, write, and execute are granted to the command.

Scope	Configures rules. This field is set to the following values: • **command**: command-based rules • **feature**: feature-based rules • **feature-group**: feature-group-based rules
Entity	Rule entity.

Notifications

N/A

Platform Description

N/A

Related Commands

- **role name**

1.12 show role feature

Function

Run the **show role feature** command to display the basic information or details about a specific feature or all features.

Syntax

show role feature [{ **detail** | **name** *feature-name* }]

Parameter Description

detail: Displays the details about all features.

name *feature-name*: Displays the basic information about a specific feature.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the basic information or details about a specific feature or all features.

Examples

The following example displays the basic information about all features.

```
Hostname> enable
Hostname# show role feature
Feature: aaa                          (Aaa related commands)
Feature: bfd                          (Bfd related commands)
```

```
Feature: bgp                          (Bgp related commands)
Feature: bridge                        (Bridge related commands)
Feature: ce-mgmt                       (Ce mgmt related commands)
```

Table 1-2 Output Fields of the show role feature Command

Field	Description
Feature	Name of a feature

The following example displays the details about all features.

```
Hostname> enable
Hostname# show role feature detail
Feature: aaa                          (Aaa related commands)
  undebug username    (W)
  undebug aaa *    (W)
  debug username    (W)
  debug aaa *    (W)
  clear aaa *    (W)
  username *    (W)
  show aaa *    (R)
  configure ; username *    (W)
  configure ; aaa *    (W)
  configure ; aaa domain * ; authentication *    (W)
  configure ; aaa domain * ; accounting *    (W)
  configure ; aaa domain * ; authorization *    (W)
  configure ; aaa domain * ; state *    (W)
  configure ; aaa domain * ; username-format *    (W)
  configure ; aaa domain * ; access-limit *    (W)
Feature: bfd                          (Bfd related commands)
  undebug bfd *    (W)
  debug bfd *    (W)
  show sbfd *    (R)
  show bfd *    (R)
  configure ; sbfd *    (W)
  configure ; bfd *    (W)
  configure ; interface * ; bfd *    (W)
```

Table 1-3 Output Fields of the show role feature detail Command

Field	Description
Feature	Name of a feature
(W)	Write command
(R)	Read command

(X)	Execution command

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show role feature-group

Function

Run the **show role feature-group** command to display the basic information or details about a specific feature group or all feature groups.

Syntax

show role feature-group [{ **detail** | **name** *group-name* [**detail**] }]

Parameter Description

detail: Displays the details about all feature groups.

name *group-name*: Displays the basic information about a specific feature group.

detail: Displays the details about a specific feature group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the basic information or details about a specific feature group or all feature groups.

Examples

The following example displays the basic information about the feature group **test**.

```
Hostname> enable
Hostname# show role feature-group name test
Feature group: test
Feature: aaa                          (Aaa related commands)
Feature: snmpd                        (Snmpd related commands)
Feature: syslogd                      (Syslogd related commands)
```

Table 1-4 Output Fields of the show role feature-group name Command

Field	Description
Feature group	Name of a feature group
Feature	Name of a feature

Notifications

N/A

Platform Description

N/A

Related Commands

- **role feature-group name**

1.14 vlan policy deny

Function

Run the **vlan policy deny** command to prohibit a role from operating all VLAN resources on a device.

Run the **no** form of this command to allow a role to operate all VLAN resources on a device.

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all VLAN resources on a device.

Syntax

vlan policy deny

no vlan policy deny

default vlan policy deny

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all VLAN resources.

Examples

The following example prohibits the role **admin-role** from operating all VLAN resources.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **show role**

1.15 vrf policy deny

Function

Run the **vrf policy deny** command to prohibit a role from operating all VRF resources.

Run the **no** form of this command to allow a role to operate all VRF resources.

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all VRF resources.

Syntax

vrf policy deny

no vrf policy deny

default vrf policy deny

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all VRF resources.

Examples

The following example prohibits the role **admin-role** from operating all VRF resources.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vrf policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **show role**

1 Line Commands

Command	Function
absolute-timeout	Configure the absolute timeout time for a line.
access-class	Configure an IPv4 access control list (ACL) for login control.
accounting commands	Enable the command accounting method list for a line.
accounting exec	Configure the user EXEC accounting method list for a line.
activation-character	Configure a character to activate a null terminal session.
authorization exec	Enable EXEC authorization for a line.
autocommand	Enable automatic command execution for a line.
clear line	Clear the connection status of a line.
databits	Configure the number of data bits per character for asynchronous lines in flow communication mode.
disconnect-character	Configure the hotkey for disconnecting terminal connections.
escape-character	Configure the character for exiting a line.
exec	Allow users to access the command line interface (CLI) through the configured line.
exec-character-bits	Configure the CLI character encoding format for asynchronous lines.
flowcontrol	Configure the flow control mode for asynchronous lines.
history	Enable historical command recording or configure the number of recorded historical commands for a line.
ipv6 access-class	Configure an IPv6 ACL for login control.
length	Configure the maximum number of lines displayed on a single screen on a specified line terminal.

line	Enter the specified line configuration mode.
line maximum-vty	Configure the allowed maximum number of VTY connections.
line vty	Increase the number of available VTY connections.
location	Configure a location description for a specific line.
monitor	Enable logging on terminals.
parity	Configure the parity bit for asynchronous lines.
privilege level	Configure the privilege level for line-based login.
refuse-message	Configure the prompt for refusing line-based login.
role	Configure a role for a line.
show history	Display historical command records of a line.
show line	Display configurations of a line.
show privilege	Display the privilege level of a line.
show users	Display login user information of a line.
speed	Configure the baud rate for a specific line terminal.
start-character	Configure the start character for software flow control for asynchronous lines.
stop-character	Configure the stop character for software flow control for asynchronous lines.
stopbits	Configure the number of stop bits in each byte transmitted through asynchronous lines.
terminal-type	Configure the type of terminals simulated by an asynchronous line terminal.
terminal databits	Configure the number of data bits per character for the current terminal in flow communication mode.
terminal escape-character	Configure the character for exiting the current terminal.
terminal exec-character-bits	Configure the CLI character encoding format for the current terminal.
terminal flowcontrol	Configure the flow control mode for the current terminal.

terminal history	Enable historical command recording or configure the number of recorded historical commands for the line connected to the current terminal.
terminal length	Configure the maximum number of lines displayed in a single screen on the current terminal.
terminal location	Configure location description of the current terminal.
terminal parity	Configure the parity bit for the asynchronous line corresponding to the current terminal.
terminal speed	Configure the baud rate for the current terminal.
terminal start-character	Configure the start character for software flow control for the current terminal.
terminal stop-character	Configure the stop character for software flow control for the current terminal.
terminal stopbits	Configure the number of stop bits in each byte transmitted through the current terminal.
terminal terminal-type	Configure other types of terminals simulated on the current terminal.
terminal width	Configure the maximum number of columns displayed in a single line on the current terminal, that is, the line width.
timeout login response	Configure the authentication timeout time for line-based login.
transport input	Configure the communication protocols supported by a line.
vacant-message	Configure a prompt for line-based logout.
width	Configure the maximum number of columns displayed in a single line for the specified line, that is, the line width.

1.1 absolute-timeout

Function

Run the **absolute-timeout** command to configure the absolute timeout time for a line.

Run the **no** form of this command to restore the default configuration.

No absolute timeout time is configured for a line by default.

Syntax

absolute-timeout *absolute-timeout-time*

no absolute-timeout

Parameter Description

absolute-timeout-time: Absolute timeout time of a line in minutes. The range is from 0 to 60, and the default value is **10**.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

After absolute timeout time is configured for a line, the line is disconnected once the specified time expires no matter whether you are operating the terminal. Before the line is disconnected, the system displays the remaining time after which the terminal will exit.

```
Terminal will be login out after 20 second
```

Examples

The following example sets the absolute timeout time of the console line to 2 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# absolute-timeout 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 access-class

Function

Run the **access-class** command to configure an IPv4 access control list (ACL) for login control.

Run the **no** form of this command to remove this configuration.

No IPv4 ACL is configured for login control by default.

Syntax

access-class { *acl-number* | *acl-name* } { **in** | **out** }

no access-class { *acl-number* | *acl-name* } { **in** | **out** }

Parameter Description

acl-number: ACL ID. Value range:
Standard IP ACLs: 1–99 or 1300–1999; Extended IP ACLs: 100–199 or 2000–2699

acl-name: ACL name.

in: Filters inbound connections.

out: Filters outbound connections.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an ACL numbered 20 to filter connections from virtual type terminal (VTY) lines 0 to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# access-class 20 in
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 accounting commands

Function

Run the **accounting commands** command to enable the command accounting method list for a line.

Run the **no** form of this command to remove this configuration.

No command accounting method list is configured for a line by default.

Syntax

accounting commands { **default** | *list-name* }

no accounting commands

Parameter Description

default: Specifies the name of the default authentication method list.

list-name: Name of the optional method list.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

- When this command is used together with Authentication, Authorization and Accounting (AAA) authentication, you need to configure AAA command accounting methods and then apply the methods to the terminal line for command accounting.
- When the role-based access control (RBAC) function is enabled, no privilege level needs to be configured for command accounting.

Examples

The following example enables command accounting for VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting commands default start-stop group tacacs+
Hostname(config)# line vty 1
Hostname(config-line)# accounting commands default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 accounting exec

Function

Run the **accounting exec** command to configure the user EXEC accounting method list for a line.

Run the **no** form of this command to remove this configuration.

No user EXEC accounting method list is configured for a line by default.

Syntax

accounting exec { **default** | *list-name* }

no accounting exec

Parameter Description

default: Specifies the name of the default authentication method list.

list-name: Name of the optional method list.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

When this command is used together with AAA authentication, you need to configure AAA user access accounting methods and then apply the methods to the VTY lines for user access accounting.

Examples

The following example sets the user EXEC accounting method list to the default method list for VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting exec default start-stop group radius
Hostname(config)# line vty 1
Hostname(config-line)# accounting exec default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 activation-character

Function

Run the **activation-character** command to configure a character to activate a null terminal session.

Run the **no** form of this command to remove this configuration.

The default character for activating a terminal session is the carriage return character (ASCII value 13).

Syntax

activation-character *ascii-value*

no activation-character

Parameter Description

ascii-value: ASCII value of the hotkey character for activating a terminal session. The range is from 0 to 127.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

If auto-selection of the terminal session activation character is enabled for the current line, the hotkey character for activating a terminal session must be set to the default value.

Examples

The following example sets the character for activating a terminal session of the console port to **Ctrl+Y** (ASCII value 25).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# activation-character 25
Hostname(config-line)# end
Hostname# exit
Press CTRL+y to get started
Hostname>
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 authorization exec

Function

Run the **authorization exec** command to enable EXEC authorization for a line.

Run the **no** form of this command to remove this configuration.

The EXEC authorization function is disabled by default.

Syntax

authorization exec { **default** | *list-name* }

no authorization exec

Parameter Description

default: Specifies the name of the default authentication method list.

list-name: Name of the optional method list.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

When this command is used together with AAA authentication, you need to configure AAA EXEC authorization methods and then apply the methods to the VTY lines for EXEC authorization.

Examples

The following example enables EXEC authorization for VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
Hostname(config)# aaa authorization exec default group radius
Hostname(config)# line vty 1
Hostname(config-line)# authorization exec default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 autocommand

Function

Run the **autocommand** command to enable automatic command execution for a line.

Run the **no** form of this command to disable this feature.

The automatic command execution function is disabled by default.

Syntax

autocommand *autocommand-command*

no autocommand

Parameter Description

autocommand-command: Command lines that are automatically executed.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

After a user acts as a dumb terminal to connect to the device through an asynchronous serial port, the user can remotely log in to the specified host by running the **telnet** command or obtain the specified application-based terminal service by running the **autocommand** command.

Examples

The following example enables automatic command execution for VTY 0 and automatically establishes a telnet connection to the terminal whose IP address is 192.168.21.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# autocommand telnet 192.168.21.100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 clear line

Function

Run the **clear line** command to clear the connection status of a line.

Syntax

clear line { **console** *console-line-number* | **vty** *vty-line-number* | *line-number* }

Parameter Description

console *console-line-number*: Clears the console connection status of a line. The value is 0.

vty *vty-line-number*: Clears the connection status of a VTY line. The range is from 0 to 35.

line-number: Line whose connection status is to be cleared. The range is from 0 to 36.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When this command is used to clear the connection status of a line, the terminal connected to the line is forcibly disconnected, and the line is restored to the idle state and can connect to a terminal again.

Examples

The following example clears the connection status of VTY 13. Client connections (such as telnet and SSH connections) on the VTY line are disconnected immediately.

```
Hostname> enable
Hostname# clear line vty 13
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 databits

Function

Run the **databits** command to configure the number of data bits per character for asynchronous lines in flow communication mode.

Run the **no** form of this command to restore the default configuration.

The default number of data bits per character for asynchronous lines in flow communication mode is **8**.

Syntax

databits *bit*

no databits

Parameter Description

bit: Number of data bits per character. The range is from 5 to 8.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

The asynchronous hardware (such as an asynchronous serial port and AUX port) of the device generates seven data bits with parity check in flow communication mode. If parity is generated, specify seven data bits per character. If no parity is generated, specify eight data bits per character. Only early devices support five or six data bits, which are seldom used.

Examples

The following example sets the number of data bits per character for the asynchronous line corresponding to the console port in flow communication mode to **7**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# databits 7
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 disconnect-character

Function

Run the **disconnect-character** command to configure the hotkey for disconnecting terminal connections.

Run the **no** form of this command to restore the default configuration.

The default hotkey for disconnecting terminal connections is **Ctrl+D** (ASCII value 4).

Syntax

disconnect-character *ascii-value*

no disconnect-character

Parameter Description

ascii-value: ASCII value of the hotkey for disconnecting terminal connections. The range is from 0 to 255.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the hotkey for disconnecting terminal connections based on requirements. The hotkey for disconnecting terminal connections cannot be common ASCII values (such as a–z, A–Z, and 0–9). Otherwise, the terminal service may be abnormal.

Examples

The following example sets the hotkey for disconnecting terminal connections on VTY lines 0 to 5 to **Ctrl+E** (ASCII value 5).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# disconnect-character 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 escape-character

Function

Run the **escape-character** command to configure the character for exiting a line.

Run the **no** form of this command to restore the default configuration.

The default character for exiting a line is **Ctrl+Shift+6** (ASCII value 30).

Syntax

escape-character *escape-value*

no escape-character

Parameter Description

escape-value: ASCII value of the user-defined character for exiting a line. The range is from 0 to 255.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

If the **escape-character** *escape-value* command is configured, you can press the combination keys specified by *escape-value* and then press **x** to terminate the current session and return to the source session that creates the current session.

Examples

The following example sets the character for exiting VTY 0 to **Ctrl+W** (ASCII value 23).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# escape-character 23
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 exec

Function

Run the **exec** command to allow users to access the command line interface (CLI) through the configured line.

Run the **no** form of this command to remove this configuration.

Users are allowed to access the CLI through configured lines by default.

Syntax

exec

no exec

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

After the **no exec** command is configured, users cannot access the CLI through the configured line. Instead, users can access CLI only through the other lines.

Examples

The following example prevents users from accessing the CLI through VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# no exec
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 exec-character-bits

Function

Run the **exec-character-bits** command to configure the CLI character encoding format for asynchronous lines.

Run the **no** form of this command to restore the default configuration.

The default CLI character encoding format is a full 8-bit ASCII character set.

Syntax

exec-character-bits { **7** | **8** }

no exec-character-bits

Parameter Description

7: Selects a 7-bit ASCII character set as the CLI character set.

8: Selects an 8-bit ASCII character set as the CLI character set.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

To enter Chinese characters or display Chinese characters, images, or other international characters in the CLI, run the **exec-character-bits 8** command.

Examples

The following example sets the CLI character encoding format for the asynchronous line corresponding to the console port to a 7-bit character set.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# exec-character-bits 7
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 flowcontrol

Function

Run the **flowcontrol** command to configure the flow control mode for asynchronous lines.

Run the **no** form of this command to restore the default configuration.

No flow control is configured for asynchronous lines by default.

Syntax

flowcontrol { **hardware** | **none** | **software** }

no flowcontrol { **hardware** | **none** | **software** }

Parameter Description

hardware: Configures hardware flow control.

none: Configures no flow control.

software: Configures software flow control.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

- The device provides the following two flow control modes:
  - Software flow control, also called soft flow controls, which uses the control keys for operations. The start and stop characters for this mode are configured by the **start-character** and **stop-character** commands respectively. The default start character is **Ctrl+Q** (XON, ASCII value 17), and the default stop character is **Ctrl+S** (XOFF, ASCII value 19).
  - Hardware flow control, also called hard flow control, which uses hardware for operations.
- By running this command, you can configure the flow control mode to keep the Tx rate of one end the same as the Rx rate of the peer end.
- Since terminals cannot receive data while sending data, flow control can prevent data loss.
- When high-speed data processing devices communicate with low-speed data processing devices (for example, a printer communicates with a network port), you also need to configure flow control to prevent data loss.

Examples

The following example configures software flow control for the asynchronous line corresponding to the console port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# flowcontrol software
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **start-character**
- **stop-character**

1.15 history

Function

Run the **history** command to enable historical command recording or configure the number of recorded historical commands for a line.

Run the **no history** command to disable the historical command recording function.

Run the **no history size** command to restore the default number of recorded historical commands.

The historical command recording function is enabled by default, and the default number of recorded historical commands is **10**.

Syntax

history [**size** *size*]

no history

no history size

Parameter Description

size *size*: Configures the number of recorded historical commands for a line. *size* indicates the number of recorded historical commands of a line. The range is from 0 to 256.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of recorded historical commands to **20** for lines 0 to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# history size 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ipv6 access-class

Function

Run the **ipv6 access-class** command to configure an IPv6 ACL for login control.

Run the **no** form of this command to remove this configuration.

No IPv6 ACL is configured for login control by default.

Syntax

ipv6 access-class { *acl-number* | *acl-name* } { **in** | **out** }

no ipv6 access-class { *acl-number* | *acl-name* } { **in** | **out** }

Parameter Description

acl-number: ACL ID. Value range:
Standard IP ACLs: 1–99 or 1300–1999; Extended IP ACLs: 100–199 or 2000–2699

acl-name: ACL name.

in: Filters inbound connections.

out: Filters outbound connections.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an ACL named **test** to filter outbound IPv6 connections of VTY lines 0 to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 4
Hostname(config-line)# ipv6 access-class test out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 length

Function

Run the **length** command to configure the maximum number of lines displayed on a single screen on a specified line terminal.

Run the **no** form of this command to restore the default configuration.

The maximum number of lines displayed on a single screen is **24** by default.

Syntax

length *screen-length*

no length

Parameter Description

screen-length: Maximum number of lines displayed on a single screen. The range is from 0 to 512. The value **0** indicates that the number of lines displayed on a single screen is not limited.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of lines displayed on a single screen to **10** for VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# length 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 line

Function

Run the **line** command to enter the specified line configuration mode.

Syntax

line { **console** | **vty** } *first-line* [*last−line*]

Parameter Description

console: Specifies the console port.

vty: Specifies a virtual terminal line, which supports a telnet or SSH connection.

first-line: ID of the first line.

last-line: ID of the last line. If it is not specified, you access only the first line.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enters the line configuration mode of VTY lines 1 to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1 3
Hostname(config-line)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 line maximum-vty

Function

Run the **line maximum-vty** command to configure the allowed maximum number of VTY connections.

Run the **no** form of this command to restore the default configuration.

The allowed maximum number of VTY connections is **36** by default.

Syntax

line maximum-vty *max-number*

no line maximum-vty

Parameter Description

max-number: Allowed maximum number of VTY connections. The range is from 0 to 36.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure the allowed maximum number of VTY connections. If the allowed maximum number of VTY terminals is set to **0**, all remote connections (including telnet, SSH, and session connections) fail. If the allowed maximum number of VTY connections is smaller than the number of online remote connections, the configuration fails and a prompt is displayed.
- The allowed maximum number of VTY connections and the number of available VTY connections are separately managed. A remote connection is established successfully only when both conditions are met.

Examples

The following example sets the allowed maximum number of VTY connections to **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line maximum-vty 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 line vty

Function

Run the **line vty** command to increase the number of available VTY connections.

Run the **no** form of this command to reduce the number of available VTY connections.

Syntax

line vty *line-number*

no line vty *line-number*

Parameter Description

line-number: Number of available VTY connections. The range is from 0 to 35.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example increases the number of available VTY connections to **20**. The available VTY connection number ranges from 0 to 19.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 19
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 location

Function

Run the **location** command to configure a location description for a specific line.

Run the **no** form of this command to restore the default configuration.

No location description is configured by default.

Syntax

location *location*

no location

Parameter Description

location: Location description of the current line.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the location description of VTY 0 to **Switch's Line Vty 0**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# location Swtich's Line Vty 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 monitor

Function

Run the **monitor** command to enable logging on terminals.

Run the **no** form of this command to remove this configuration.

The logging function is disabled by default.

Syntax

monitor

no monitor

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables logging on terminals connected to VTY lines 0-5.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# monitor
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 parity

Function

Run the **parity** command to configure the parity bit for asynchronous lines.

Run the **no** form of this command to restore the default configuration.

No parity bit is configured for asynchronous lines by default.

Syntax

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

no parity

Parameter Description

even: Specifies even parity check.

none: Specifies no parity check.

odd: Specifies odd parity check.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

When using certain hardware (such as a console port) for communication, you usually need to configure a parity bit.

Examples

The following example configures even parity check for the asynchronous line corresponding to the console port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# parity even
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.24 privilege level

Function

Run the **privilege level** command to configure the privilege level for line-based login.

Run the **no** form of this command to restore the default configuration.

The default privilege level for line-based login is **1**.

Syntax

privilege level *privilege-level*

no privilege level

Parameter Description

privilege-level: Privilege level for line-based login. The range is from 0 to 15.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

This command is unavailable when the RBAC function is enabled.

Examples

The following example sets the privilege level of login through VTY lines 0-4 to **14**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 4
Hostname(config-line)# privilege level 14
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 refuse-message

Function

Run the **refuse-message** command to configure the prompt for refusing line-based login.

Run the **no** form of this command to remove this configuration.

No prompt is configured for refusing line-based login by default.

Syntax

refuse-message [*c message c*]

no refuse-message

Parameter Description

c message c: Prompt for refusing line-based login. *c* indicates the prompt delimiter, which is any character. *message* indicates the prompt content. Delimiters are not allowed in the prompt content.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure the prompt for refusing line-based login. Any characters following the ending delimiter are dropped.
- When a user is refused to log in to the device, a prompt appears, indicating that the current line refuses the user's login.

Examples

The following example sets the prompt for refusing line-based login to **Illegal users are not allowed to log in to the device**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config-line)#refuse-message @ Illegal users are not allowed to log in to the device @
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 role

Function

Run the **role** command to configure a role for a line.

Run the **no** form of this command to remove this configuration.

A role is configured for each line by default. The default role for the console line is **network-admin**, and the default role for VTY lines is **network-operator**.

Syntax

role *role-name*

no role *role-name*

Parameter Description

role-name: Role name.

Command Modes

Line configuration mode

Default Level

15

Usage Guidelines

- This command is used to configure a role for a line.
- Each line can be configured with 1 to 64
- roles. The last role cannot be deleted. If it is deleted, a failure prompt is displayed.

Examples

The following example configures role **priv-0** for VTY 1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# line vty 1
Hostname(config-line)# role priv-0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show history

Function

Run the **show history** command to display historical command records of a line.

Syntax

show history

Parameter Description

all-users: Displays historical command records of all terminal users.

Command Modes

All modes except the User EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays historical command records of the current line.

```
Hostname> enable
Hostname# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

Table 1-1 Output Fields of the show history Command

Field	Description
exec	Command mode for executing this command

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show line

Function

Run the **show line** command to display configurations of a line.

Syntax

show line { **console** *console-line-number* | **vty** *vty-line-number* | *line-number* }

Parameter Description

console *console-line-number*: Displays configurations of the console line. The *console-line number* value is 0.

vty *vty-line-number*: Displays configurations of a VTY line. *vty-line-num* indicates the VTY line ID. The range is from 0 to 35.

line-number: Line number. The range is from 0 to 36.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays configurations of the console line.

```
Hostname> enable
Hostname# show line console 0
```

```
CON    Type    speed   Overruns
* 0    CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
            ^^x    none       ^M
Timeouts:     Idle EXEC    Idle Session
            never       never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output:  395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

Table 1-2 Output Fields of the show line Command

Field	Description
CON	Terminal type ● **CON** indicates the console. ● **0** indicates the terminal line ID. ● The ID with an asterisk (*) indicates the terminal line in use.
Type	Terminal type, including CON and VTY.
speed	Asynchronous speed
Overruns	Count of overrun errors received by the driver
Line 0	Terminal line ID
Location: ""	Line location
Type: "vt100"	Compatible terminal standard of a line
Special Chars	Special terminal characters, including the **Escape**, **Disconnect**, and **Activation** characters
Timeouts	Timeout time of a terminal session. **never** indicates that a session never times out.
History	Historical command recording function and the maximum number of recorded historical commands.
Total input	Count of data received from the driver
Total output	Count of data sent to the driver
Data overflow	Count of received data that overflows
stop rx interrupt	Count of RX interrupts of the driver

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show privilege

Function

Run the **show privilege** command to display the privilege level of a line.

Syntax

show privilege

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the privilege level of the current line.

```
Hostname> enable
Hostname# show privilege
Current privilege level is 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 show users

Function

Run the **show users** command to display login user information of a line.

Syntax

show users [**all**]

Parameter Description

all: Displays information about all available line users, including login users and logout users.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about login users.

```
Hostname> enable
Hostname# show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- -------------------
   0 con 0      -         idle               00:00:46  None
   1 vty 0      -         idle               00:00:29   20.1.1.2
*  2 vty 1      -         idle               00:00:00   20.1.1.2
```

Table 1-3 Output Fields of the show users Command

Field	Description
Line	ID of a login line
User	Username
Host(s)	User IP address
Idle	User terminal timeout time
Location	Local IP address used for login

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 speed

Function

Run the **speed** command to configure the baud rate for a specific line terminal.

Run the **no** form of this command to restore the default configuration.

The default baud rate is 9600 bps.

Syntax

speed *baudrate*

no speed

Parameter Description

baudrate: Baud rate of a line terminal in bps. The range is from 9600 to 115200. For serial interfaces, the baud rate is **9600** , **19200**, **38400**, **57600**, or **115200**.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the baud rate of VTY 1 to 115200 bps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# speed 115200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 start-character

Function

Run the **start-character** command to configure the start character for software flow control for asynchronous lines.

Run the **no** form of this command to restore the default configuration.

The default start character for software flow control for asynchronous lines is **Ctrl+Q** (ASCII value 17).

Syntax

start-character *ascii-value*

no start-character

Parameter Description

ascii-value: ASCII value of the start character for software flow control for asynchronous lines. The range is from 0 to 255.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

After software flow control is enabled for an asynchronous line, the start character indicates the start of data transmission.

Examples

The following example sets the start character for software flow control for the asynchronous line corresponding to the console port to **Ctrl+Y** (ASCII value 25).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# start-character 25
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 stop-character

Function

Run the **stop-character** command to configure the stop character for software flow control for asynchronous lines.

Run the **no** form of this command to restore the default configuration.

The default stop character for software flow control for asynchronous lines is **Ctrl+S** (ASCII value 19).

Syntax

stop-character *ascii-value*

no stop-character

Parameter Description

ascii-value: ASCII value of the stop character for software flow control for asynchronous lines. The range is from 0 to 255.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

After software flow control is enabled for an asynchronous line, the stop character indicates the end of data transmission.

Examples

The following example sets the stop character for software flow control for the asynchronous line corresponding to the console port to **Ctrl+Z** (ASCII value 26).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# stop-character 26
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 stopbits

Function

Run the **stopbits** command to configure the number of stop bits in each byte transmitted through asynchronous lines.

Run the **no** form of this command to restore the default configuration.

The default number of stop bits in each byte transmitted through asynchronous lines is **2**.

Syntax

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

no stopbits

Parameter Description

1: Configures one stop bit.

2: Configures two stop bits.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

You should configure the stop bits for communication between an asynchronous line and the connected asynchronous device (such as a conventional numb terminal and modem).

Examples

The following example sets the number of stop bits in each byte transmitted through the asynchronous line corresponding to the console port to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# stopbits 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 terminal-type

Function

Run the **terminal-type** command to configure the type of terminals simulated by an asynchronous line terminal.

Run the **no** form of this command to restore the default configuration.

The default terminal type is **vt100**.

Syntax

terminal-type *terminal-type-string*

no terminal-type

Parameter Description

terminal-type-string: Description of the terminal type, such as **vt100** and **ansi**.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

You can run the **terminal-type vt100** command to restore the default terminal type. In telnet connection scenarios, you can run this command to configure other types of terminals simulated on the terminal connected to a line as required. Upon telnet connection, one end negotiates with the other end about the terminal type based on its terminal type configuration (telnet option negotiation ID: 0x18). For details, see RFC 854.

Examples

The following example sets the type of terminals simulated by the asynchronous line terminal corresponding to the console port to **ansi**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# terminal-type ansi
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 terminal databits

Function

Run the **terminal databits** command to configure the number of data bits per character for the current terminal in flow communication mode.

Run the **no** form of this command to restore the default configuration.

The default number of data bits per character for the current terminal in flow communication mode is **8**.

Syntax

terminal databits *bit*

terminal no databits

Parameter Description

bit: Number of data bits per character. The range is from 5 to 8.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of data bits per character for the current terminal in flow communication mode to **7**.

```
Hostname> enable
Hostname# terminal databits 7
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.37 terminal escape-character

Function

Run the **terminal escape-character** command to configure the character for exiting the current terminal.

Run the **no** form of this command to restore the default configuration.

The default character for exiting the current terminal is **Ctrl+Shift+6** (ASCII value 30).

Syntax

terminal escape-character *escape-value*

terminal no escape-character

Parameter Description

escape-value: ASCII value in decimal notation of the user-defined character for exiting the current terminal. The range is from 0 to 255.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **escape-character** *escape-value* command is configured, you can press the combination keys specified by *escape-value* and then press **x** to terminate the current session and return to the source session that creates the current session.

Examples

The following example sets the character for exiting the current terminal to **Ctrl+W** (ASCII value 23).

```
Hostname> enable
Hostname# terminal escape-character 23
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.38 terminal exec-character-bits

Function

Run the **terminal exec-character-bits** command to configure the CLI character encoding format for the current terminal.

Run the **no** form of this command to restore the default configuration.

The default CLI character encoding format is a full 8-bit ASCII character set.

Syntax

terminal exec-character-bits { **7** | **8** }

terminal no exec-character-bits

Parameter Description

7: Selects a 7-bit ASCII character set as the CLI character set.

8: Selects an 8-bit ASCII character set as the CLI character set.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If you need to enter Chinese characters or display Chinese characters, images, or other international characters in the CLI, run the **terminal exec-character-bits 8** command.

Examples

The following example sets the CLI character encoding format for the current terminal to a 7-bit character set.

```
Hostname> enable
Hostname# terminal exec-character-bits 7
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 terminal flowcontrol

Function

Run the **terminal flowcontrol** command to configure the flow control mode for the current terminal.

Run the **no** form of this command to restore the default configuration.

No flow control is configured for the current terminal by default.

Syntax

terminal flowcontrol { **hardware** | **none** | **software** }

terminal no flowcontrol { **hardware** | **none** | **software** }

Parameter Description

hardware: Configures hardware flow control.

none: Configures no flow control.

software: Configures software flow control.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures software flow control for the current terminal.

```
Hostname> enable
Hostname# terminal flowcontrol software
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 terminal history

Function

Run the **terminal history** command to enable historical command recording or configure the number of recorded historical commands for the line connected to the current terminal.

Run the **terminal no history** command to disable the historical command recording function for the line connected to the current terminal.

Run the **terminal no history size** command to restore the default number of recorded historical commands for the line connected to the current terminal.

The historical command recording function is enabled by default, and the default number of recorded historical commands is **10**.

Syntax

terminal history [**size** *size*]

terminal no history

terminal no history size

Parameter Description

size *size*: Configures the maximum number of recorded historical commands for a line. *size* indicates the maximum number of recorded historical commands of a line. The range is from 0 to 256.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of recorded historical commands for the line connected to the current terminal to **20**.

```
Hostname> enable
Hostname# terminal history size 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 terminal length

Function

Run the **terminal length** command to configure the maximum number of lines displayed in a single screen on the current terminal.

Run the **no** form of this command to restore the default configuration.

The maximum number of lines displayed in a single screen is **24** by default.

Syntax

terminal length *screen-length*

terminal no length

Parameter Description

screen-length: Maximum number of lines displayed in a single screen. The range is from 0 to 512. The value **0** indicates that the number of lines displayed in a single screen is not limited.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of lines displayed in a single screen on the current terminal to **10**.

```
Hostname> enable
Hostname# terminal length 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 terminal location

Function

Run the **terminal location** command to configure location description of the current terminal.

Run the **no** form of this command to restore the default configuration.

No location description is configured for the current terminal by default.

Syntax

terminal location *location*

terminal no location

Parameter Description

location: Location description of the current terminal.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets location description of the current terminal to **Switch's Line Vty 0**.

```
Hostname> enable
Hostname# terminal location Swtich’s Line Vty 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 terminal parity

Function

Run the **terminal parity** command to configure the parity bit for the asynchronous line corresponding to the current terminal.

Run the **no** form of this command to restore the default configuration.

No parity bit is configured for the asynchronous line corresponding to the current terminal by default.

Syntax

terminal parity { **even** | **none** | **odd** }

terminal no parity

Parameter Description

even: Specifies even parity check.

none: Specifies no parity check.

odd: Specifies odd parity check.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When using certain hardware (such as a console port) for communication, you usually need to configure a parity bit.

Examples

The following example configures even parity check for the asynchronous line corresponding to the current terminal.

```
Hostname> enable
Hostname# terminal parity even
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 terminal speed

Function

Run the **terminal speed** command to configure the baud rate for the current terminal.

Run the **no** form of this command to restore the default configuration.

The default baud rate of the current terminal is 9600 bps.

Syntax

terminal speed *baudrate*

terminal no speed

Parameter Description

baudrate: Baud rate of a line terminal in bps. The range is from 9600 to 115200. For serial interfaces, the baud rate is **9600**, **19200**, **38400**, **57600**, or **115200**.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the baud rate of the current terminal to 115,200 bps.

```
Hostname> enable
Hostname# terminal speed 115200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 terminal start-character

Function

Run the **terminal start-character** command to configure the start character for software flow control for the current terminal.

Run the **no** form of this command to restore the default configuration.

The default start character for software flow control for the current terminal is **Ctrl+Q** (ASCII value 17).

Syntax

terminal start-character *ascii-value*

terminal no start-character

Parameter Description

ascii-value: ASCII value of the start character for software flow control for the current terminal. The range is from 0 to 255.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the start character for software flow control for the current terminal to **Ctrl+Y** (ASCII value 25).

```
Hostname> enable
Hostname# terminal start-character 25
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 terminal stop-character

Function

Run the **terminal stop-character** command to configure the stop character for software flow control for the current terminal.

Run the **no** form of this command to restore the default configuration.

The default stop character for software flow control for the current terminal is **Ctrl+S** (ASCII value 19).

Syntax

terminal stop-character *ascii-value*

terminal no stop-character

Parameter Description

ascii-value: ASCII value of the stop character for software flow control for the current terminal. The range is from 0 to 255.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the stop character for software flow control for the current terminal to **Ctrl+Z** (ASCII value 26).

```
Hostname> enable
Hostname# terminal stop-character 26
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 terminal stopbits

Function

Run the **terminal stopbits** command to configure the number of stop bits in each byte transmitted through the current terminal.

Run the **no** form of this command to restore the default configuration.

The default number of stop bits in each byte transmitted through the current terminal is **2**.

Syntax

terminal stopbits { **1** | **2** }

terminal no stopbits

Parameter Description

1: Configures one stop bit.

2: Configures two stop bits.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of stop bits in each byte transmitted through the current terminal to **1**.

```
Hostname> enable
Hostname# terminal stopbits 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.48 terminal terminal-type

Function

Run the **terminal terminal-type** command to configure other types of terminals simulated on the current terminal.

Run the **no** form of this command to restore the default configuration.

The default terminal type is **vt100**.

Syntax

terminal terminal-type *terminal-type-string*

terminal no terminal-type

Parameter Description

terminal-type-string: Description of the terminal type, such as **vt100** and **ansi**.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets other types of terminals simulated on the current terminal to **ansi**.

```
Hostname> enable
Hostname# terminal terminal-type ansi
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 terminal width

Function

Run the **terminal width** command to configure the maximum number of columns displayed in a single line on the current terminal, that is, the line width.

Run the **no** form of this command to restore the default configuration.

The maximum number of columns displayed in a single line is **79** by default.

Syntax

terminal width *screen-width*

terminal no width

Parameter Description

screen-width: Maximum number of columns displayed in a single line. The range is from 0 to 256.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of columns displayed in a single line on the current terminal to **10**.

```
Hostname> enable
Hostname# terminal width 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 timeout login response

Function

Run the **timeout login response** command to configure the authentication timeout time for line-based login.

Run the **no** form of this command to restore the default configuration.

The default authentication timeout time for line-based login is 30 seconds.

Syntax

timeout login response *response-timeout-time*

no timeout login response

Parameter Description

response-timeout-time: Authentication timeout time for line-based login in seconds. The range is from 1 to 300.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the authentication timeout time for login of VTY lines 0-5 to 300 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# timeout login response 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 transport input

Function

Run the **transport input** command to configure the communication protocols supported by a line.

Run the **no** form of this command to restore the default configuration.

All communication protocols are supported by default. That is, both SSH and telnet are supported.

Syntax

transport input { **all** | **ssh** | **telnet** | **none** }

no transport input { **all** | **ssh** | **telnet** | **none** }

Parameter Description

all: Specifies that all communication protocols are supported in a line.

ssh: Specifies that the SSH protocol is supported for communication in a line.

telnet: Specifies that the telnet protocol is supported for communication in a line.

none: Specifies that no protocol is supported for communication in a line.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example allows only the telnet protocol in VTY lines 0 to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0 5
Hostname(config-line)# transport input ssh
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 vacant-message

Function

Run the **vacant-message** command to configure a prompt for line-based logout.

Run the **no** form of this command to remove this configuration.

No prompt information is configured for line-based logout by default.

Syntax

vacant-message [*c message c*]

no vacant-message

Parameter Description

c message c: Prompt for logout. *c* indicates the prompt delimiter, which can be any character. *message* indicates the prompt content. Delimiters are not allowed in the prompt content.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure the prompt for line-based logout. Any characters following the ending delimiter are dropped.
- When a user logs out of the device, a prompt appears, indicating that the current line logs out.

Examples

The following example sets the prompt for line-based logout through VTY 1 to **Exit device**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# vacant-message @ Exit device @
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 width

Function

Run the **width** command to configure the maximum number of columns displayed in a single line for the specified line, that is, the line width.

Run the **no** form of this command to restore the default configuration.

The maximum number of columns displayed in a line is **79** by default.

Syntax

width *screen-width*

no width

Parameter Description

screen-width: Maximum number of columns displayed in a single line. The range is from 0 to 256.

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the line width to 10 columns for VTY 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 1
Hostname(config-line)# width 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 File System Commands

Command	Function
cd	Change the current path or file system.
copy	Copy files between file systems.
delete	Delete one file.
dir	Display the file list in one file system.
eject	Unmount the USB device.
erase	Erase the file system.
file	Display information about a file.
file prompt	Configure the file operation prompt mode.
mkdir	Create a directory.
more	Display the content of a file.
pwd	Display the full path to the current working directory.
rename	Rename a current file or directory.
rmdir	Delete an empty directory.
show disk	Display information about the USB flash drive/flash disk.
show file systems	Display information about a file system.
show mount	Display information about the file system mounted on the device.
tftp-client source	Specify a source IP address or source interface to be used for communication between the TFTP client and the TFTP server.
verify	Compute, display, and verify Message Digest 5 (MD5) information.

1.1 cd

Function

Run the **cd** command to change the current path or file system.

The default file system is **flash:**. If no path name is specified, the current path of the specified file system is the root path.

Syntax

cd [*filesystem*:] [*directory*]

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

directory: Path name. A path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example changes the current file system to USB:.

```
Hostname> enable
Hostname# pwd
flash:/
Hostname# cd usb:
Hostname# pwd
usb:/
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **pwd**

1.2 copy

Function

Run the **copy** command to copy files between file systems.

Syntax

copy *src-url dst-url* [*vrf_name*]

copy *src-url dst-url*

Parameter Description

src-url: URL of the source file. The file can be local or remote.

dst -url: URL of the target file. The file can be local or remote.

vrf_name: Specifies the VRF. Whether this parameter is supported depends on the actual product version.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

When the file to be copied exists on the target URL, the target file system determines the action, for example, reporting an error, overwriting the file, or asking users to make the choice.

Table 1-1 Description of URL Parameters

Parameter	Description
running-config	Specifies the running configuration file.
startup-config	Specifies the configuration file for initialization.
flash:	Specifies the local flash file system.
tftp:	Specifies the URL of the Trivial File Transfer Protocol (TFTP) network server, with the syntax as follows: **tftp:**[[//location] /directory] /filename
oob_tftp: [**via mgmt** { *number* }] **oob_tftp:**	Specifies the URL of the TFTP network server connected with the out-of-band port. If there are multiple MGMT ports, you can select one. Specifies the URL of the TFTP network server connected with the out-of-band port.
ftp	Specifies the URL of the File Transfer Protocol (FTP) network server, with the syntax as follows: **ftp**:[[//[*uname* [:*passwd*] @] *location*] /*directory* **/filename**

Parameter	Description
oob_ftp: [**via mgmt.** { number }] **oob_ftp:**	Specifies the URL of the FTP network server connected with the out-of-band port. If there are multiple MGMT ports, you can select one. Specifies the URL of the FTP network server connected with the out-of-band port.
http	Specifies the URL of the Hypertext Transfer Protocol (HTTP) network server, with the syntax as follows: **http**:[[//*location*] */directory*] **/filename**
oob_http: [**via mgmt.** { *number* }] **oob_http:**	Specifies the URL of the HTTP network server connected with the out-of-band port, If there are multiple MGMT ports, you can select one. Specifies the URL of the HTTP network server connected with the out-of-band port.

Examples

The following example copies the file **netconfig** on the device with the IP address of 192.168.64.2 to **netconfig** on the flash disk.

```
Hostname> enable
Hostname# copy tftp://192.168.64.2/netconfig flash:/netconfig
Do you want to overwrite [/data/netconfig]? [Y/N]:y
Press Ctrl+C to quit
!
Copy success.
```

Notifications

N/A

Common Errors

The specified source file to be copied is a directory, which cannot be copied.

Platform Description

N/A

Related Commands

- **dir**

1.3 delete

Function

Run the **delete** command to delete one file.

The default file system is **flash:**.

Syntax

delete [*filesystem*:] *file-url*

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

file-url: File name containing the path. A file path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example deletes the file **fstab** from the flash disk.

```
Hostname> enable
Hostname# pwd
flash:/
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Hostname# delete flash:/fstab
Do you want to delete [flash:/fstab]? [Y/N]:y
Delete success.
Hostname# dir
Directory of flash:/
1   -rw-      4096   Jan 03 2012 12:32:09  rc.d
2   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
2 files, 0 directories
10,489,856 bytes total (13,192,992 bytes free)
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- dir

1.4 dir

Function

Run the **dir** command to display the file list in one file system.

The default file system is **flash:**. If no path name is specified, the current path of the specified file system is the root path.

Syntax

dir [*filesystem*:] [*file-url*]

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

file-url: Path name. A path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays a list of files in the root directory of the flash disk.

```
Hostname> enable
Hostname# dir flash:/
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Table 1-2 Output Fields of the dir Command

Field	Description
1, 2, 3 ……	Index number

Field	Description
-rw-	Permission. One file can have any of the following permissions: ● d: Directory ● r: Read ● w: Write ● x: Executable
10485760	File size
rpmdb	File name
files	Number of files
directories	Number of directories
total	Total size
free	Available space

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 eject

Function

Run the **eject** command to unmount the USB device.

Syntax

eject usb0

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example unmounts the USB device.

```
Hostname> enable
Hostname# eject ?
  usb0  Eject usb disk 0
Hostname# eject usb0
Hostname#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 erase

Function

Run the **erase** command to erase the file system.

Syntax

erase *filesystem*:

Parameter Description

filesystem:: Name of a file system.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example erases the USB file system.

```
Hostname> enable
Hostname# erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 …
Erase disk usb0 done!
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir**

1.7 file

Function

Run the **file** command to display information about a file.

The default file system is **flash:**.

Syntax

file [*filesystem*:] *file-url*

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

file-url: File name containing the path. A file name starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays information about executable file **gcc**.

```
Hostname> enable
Hostname# file flash:/gcc
/usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically
linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 file prompt

Function

Run the **file prompt** command to configure the file operation prompt mode.

The default file operation prompt mode is **noisy**.

Syntax

file prompt [**noisy** | **quiet**]

Parameter Description

Noisy: Displays a prompt for all file operations.

Quiet: Displays a prompt rarely.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the file operation prompt mode to noisy.

```
Hostname> enable
Hostname# file prompt noisy
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 mkdir

Function

Run the **mkdir** command to create a directory.

The default file system is **flash:**. If no path name is specified, the current path of the specified file system is the root path.

Syntax

mkdir [*filesystem*:] *directory*

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

directory: Path name. A path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example creates a directory named **newdir**.

```
Hostname> enable
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
Hostname# mkdir newdir
Created dir flash:/newdir
Hostname# dir
```

```
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
4   drw-      4096   Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 more

Function

Run the **more** command to display the content of a file.

The file is displayed in its original format by default.

Syntax

more [**/ascii** | **/binary**] [*filesystem*:] *file-url*

Parameter Description

/ascii: Displays the file content in the American Standard Code for Information Interchange (ASCII) format.

/binary: Displays the file content in hexadecimal notation/text format.

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

file-url: Path name. A path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the content of file **netconfig** in the root directory of the flash disk.

```
Hostname> enable
Hostname# more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#      <network_id> <semantics> <flags> <protofamily> <protoname> \
#            <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp       tpi_clts     v    inet    udp    -      N/A
tcp       tpi_cots_ord  v    inet    tcp    -      N/A
udp6      tpi_clts     v    inet6   udp    -      N/A
tcp6      tpi_cots_ord  v    inet6   tcp    -      N/A
rawip     tpi_raw      -    inet    -      -      N/A
local     tpi_cots_ord  -    loopback  -     -      N/A
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 pwd

Function

Run the **pwd** command to display the full path to the current working directory.

Syntax

pwd

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the process of switching the working directory from **flash:** to **usb:**.

```
Hostname> enable
Hostname# pwd
flash:/
Hostname# cd usb:/
Hostname# pwd
usb:/
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 rename

Function

Run the **rename** command to rename a current file or directory.

Syntax

rename *src-url dst-url*

Parameter Description

src-url:-url: Path or file name of the source file or directory to be renamed.

dst-url:-url: Path or file name of the renamed destination file or directory.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example renames the file **fstab** in the root directory of the flash disk as **new-fstab**.

```
Hostname> enable
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Hostname# rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  new-fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 rmdir

Function

Run the **rmdir** command to delete an empty directory.

The default file system is **flash:**.

Syntax

rmdir [*filesystem*:] *directory*

Parameter Description

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

directory: Name of a folder under the file system URL.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example deletes empty directory **test**.

```
Hostname> enable
Hostname# mkdir newdir
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
4   drw-      4096   Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
Hostname# rmdir newdir
removed dir flash:/newdir
Hostname# dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show disk

Function

Run the **show disk** command to display information about the USB flash drive/flash disk.

Syntax

show disk [**usb** | **flash**]

Parameter Description

usb: Displays information about the USB flash drive.

flash: Displays information about the flash disk.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about the flash disk.

```
Hostname> enable
Hostname# show disk flash
Nand flash size: 512MB
Nor flash size: 1MB
```

Table 1-3 Output Fields of the show disk flash Command

Field	Description
Nand flash size	Size of the NAND flash memory.
Nor flash size	Size of the NOR flash memory.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show file systems

Function

Run the **show file systems** command to display information about a file system.

Syntax

show file systems

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about all mounted file systems.

```
Hostname> enable
Hostname# show file systems
  Size(KB)      Free(KB)    Type   Flags  Prefixes
       NA           NA      ram    rw  tmp:
       NA           NA   network    rw  tftp:
       NA           NA   network    rw  oob_tftp:
     8192         2416     disk    rw  flash:
 167772160    147772160     disk    rw  sata0:
  1048576       548576     disk    rw  usb0:
   262144       152144     disk    rw  sd0:
```

Table 1-4 Output Fields of the show file systems Command

Field	Description
Size(KB)	Space of a file system, in KB.
Free(KB)	Available space of the file system, in KB.
Type	Type of the file system.

Field	Description
Flags	Permissions on the file system, including: ● ro: Read-only. ● wo: Write-only. ● rw: Read and write.
Prefixes	Prefix of the file system.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show mount

Function

Run the **show mount** command to display information about the file system mounted on the device.

Syntax

show mount

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays information about the file system mounted on the device.

```
Hostname> enable
Hostname# show mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
```

```
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev)
```

Table 1-5 Output Fields of the show mount Command

Field	Description
proc	Source address of the mounted file system.
/proc	Destination address of the mounted file system.
type	Mounting type.
(rw, noexec, nosuid, nodev)	Mounting property.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 tftp-client source

Function

Run the **tftp-client source** command to specify a source IP address or source interface to be used for communication between the TFTP client and the TFTP server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No source IP address or source interface is configured for communication between the TFTP client and the TFTP server by default.

Syntax

tftp-client source { **ip** *ipv4-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }

no tftp-client source { **ip** *ipv4-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }

default tftp-client source { **ip** *ipv4-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }

Parameter Description

ipv4-address: IPv4 source address.

ipv6-address: IPv6 source address.

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example specifies 192.168.23.236 as the IP address to be used for communication between the TFTP client and the TFTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tftp-client source ip 192.168.23.236
```

Notifications

If the configured IP address or interface is not a local address, an error will be reported. Otherwise, the binding will be successful without any prompt.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 verify

Function

Run the **verify** command to compute, display, and verify Message Digest 5 (MD5) information.

The default file system is **flash:**.

Syntax

verify [**/md5** *md5-value*] *filesystem:* [*file-url*]

Parameter Description

/md5: Computes and displays the MD5 value of a file.

md5-value: MD5 value of the file, which will be compared with the computed MD5 value.

filesystem:: URL of the file system, followed by a colon (:). File systems include **flash:**, **usb:**, and **tmp:**.

file-url: Path name. A path starting with "/" is an absolute path. Otherwise, it is a relative path.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example computes the MD5 value of **flash:/gcc** and makes a comparison.

```
Hostname> enable
Hostname# verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying flash:/gcc = 8b072de7db7affd8b2ef824e7e4d716c
Hostname# verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc
%Error verifying flash:/gcc
Computed signature = 8b072de7db7affd8b2ef824e7e4d716c
Submitted signature = 8b072de7db7affd8b2ef824e7e4d71
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 HTTP Commands

Command	Function
enable service web-server	Enable the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) service.
http check-version	Detect upgrade files on an HTTP server.
http port	Configure a port for the HTTP service.
http secure-port	Configure a port for the HTTPS service.
http update	Configure a file for manual upgrade.
http update mode	Configure the manual upgrade mode for HTTP upgrade.
http update server	Configure the server address and port number for HTTP upgrade.
http update set oob	Configure HTTP upgrade using the MGMT port.
http update source_ip	Configure the source IP address for HTTP upgrade.
http update time	Configure HTTP automatic detection time.
show web-server https certificate information	Display information about the HTTPS service certificate.
show web-server status	Display the configuration and status of the Web service.
webmaster level	Configure a username and a password for Web login and authentication.
web-server http redirect-to-https	Configure automatic HTTP redirection to HTTPS.
web-server https certificate	Install an HTTPS certificate.
web-server https generate self-signed-certificate	Generate an HTTPS service self-signed certificate again.

1.1 enable service web-server

Function

Run the **enable service web-server** command to enable the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) service.

Run the **no** form of this command to disable the HTTP and HTTPS service.

Run the **default** form of this command to restore the default configuration of the HTTP and HTTPS service.

The HTTP and HTTPS services are disabled by default.

Syntax

enable service web-server [**all** | **http** | **https**]

no enable service web-server [**all** | **http** | **https**]

default enable service web-server [**all** | **http** | **https**]

Parameter Description

all | **http** | **https**: Enables the service. Here, **all** indicates that both the HTTP and HTTPS services are enabled; **http** indicates that only the HTTP service is enabled; **https** indicates that only the HTTPS service is enabled. Both the HTTP and HTTPS services are enabled by default.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If no keyword is configured or the **all** keyword is configured at the end of the command, both the HTTP and HTTPS services are enabled; if the **http** keyword is configured, only the HTTP service is enabled; if the **https** keyword is configured, only the HTTPS service is enabled.
- The **no enable service web-server** command or the **default enable service web-server** command is configured to disable the HTTP service. If no keyword is entered at the end of the **no enable service web-server** or **default enable service web-server** command, both the HTTP and HTTPS services are disabled.

Examples

The following example enables both the HTTP and HTTPS services.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable service web-server all
```

Notifications

If the port is 80 and the HTTP service fails, the following notification will be displayed:

```
%notice:Failed to open tcp listen, port=[80].
```

Common Errors

If the port is occupied by other modules, the Web service may not be enabled.

Platform Description

N/A

Related Commands

N/A

1.2 http check-version

Function

Run the **http check-version** command to detect upgrade files on an HTTP server.

Detecting available upgrade files on an HTTP server is enabled by default.

Syntax

http check-version [**extend**]

Parameter Description

extend: Detects upgrade files on more than one HTTP server.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example detects upgrade files on an HTTP server.

```
Hostname> enable
Hostname# http check-version
Business modules need to be updated: character-db, route-db
app name:web
   app-name          version         filename
----- -----------------
character-db    2014.02.09.14.02.09 app_sub_1.exe
character-db    2014.02.09.14.02.09 app_file_list.txt
character-db    2014.02.09.14.02.09 app_sub_3.exe
character-db    2014.02.09.14.02.09 app_sub_2.exe
route-db       2013.12.01.00      route-choose.db
```

Notifications

If no service module is registered with the upgrade module, the following notification will be displayed:

```
%notice: No bussiness modules registration.
```

If the device cannot establish a connection with the server or the communication with the server fails, the following notification will be displayed:

```
%notice: Communicate with the server failed.
```

If the memory of the device is insufficient, the following notification will be displayed:

```
%warning: Out of memory, application memory failure.
```

If the format of the response packet of the server is incorrect, the following notification will be displayed:

```
%notice: The server response message format is wrong.
```

If the service module is being upgraded or has not registered a version number, the following notification will be displayed:

```
%notice: Suspend, some business modules are upgrading or haven't registered release.
```

If the versions of all service modules are the latest, the following notification will be displayed:

```
%notice: All bussiness modules are the latest versions.
```

Common Errors

Communication with the server fails during running of this command, possibly because the network fails or the DNS service is not enabled.

Platform Description

N/A

Related Commands

N/A

1.3 http port

Function

Run the **http port** command to configure a port for the HTTP service.

Run the **no** form of this command to restore the default port number.

The default port number of the HTTP service is **80**.

Syntax

http port *port-number*

no http port

Parameter Description

port-number: Port number of the HTTP service. The range is 80 and from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the port number of the HTTP service to 8080.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http port 8080
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 http secure-port

Function

Run the **http secure-port** command to configure a port for the HTTPS service.

Run the **no** form of this command to restore the default port number.

The default port number of the HTTPS service is **443**.

Syntax

http secure-port *port-number*

no http secure-port

Parameter Description

port-number: Port number of the HTTPS service. The range is 443 and from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the port number of the HTTPS service to 4443.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http secure-port 4443
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 http update

Function

Run the **http update** command to configure a file for manual upgrade.

No file for manual upgrade is configured by default.

Syntax

http update [**extend**] { **all** | *module* }

Parameter Description

extend: Configures multiple servers.

all: Upgrades all the service modules.

Module: Name of the service module to be upgraded. More names can be entered and are separated by spaces.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example manually downloads the latest upgrade file **route-db** from the remote server.

```
Hostname> enable
```

```
Hostname# http update route-db
Downloading updated files, please wait...
Press Ctrl+C to quit
route-db: download and notify successfully.
```

Notifications

If no service module is registered with the upgrade module, the following notification will be displayed:

```
%notice: No bussiness modules registration.
```

If the specified service module is not registered, the following notification will be displayed:

```
%notice: The bussiness modules haven't registered.
```

If the current upgrade module is being upgraded, the following notification will be displayed:

```
%notice: There are business modules in the upgrading, please wait for a moment.
```

If the device cannot establish a connection with the server or the communication with the server fails, the following notification will be displayed:

```
%notice: Communicate with the server failed.
```

If the memory of the device is insufficient, the following notification will be displayed:

```
%warning: Out of memory, application memory failure.
```

If the format of the response packet of the server is incorrect, the following notification will be displayed:

```
%notice: The server response message format is wrong.
```

If the service module is being upgraded or has not registered a version number, the following notification will be displayed:

```
%notice: Suspend, some business modules are upgrading or haven't registered release.
```

If the versions of all service modules are the latest, the following notification will be displayed:

```
%notice: All bussiness modules are the latest versions.
```

Common Errors

Communication with the server fails during running of this command, possibly because the network fails or the DNS service is not enabled.

Platform Description

N/A

Related Commands

N/A

1.6 http update mode

Function

Run the **http update mode** command to configure the manual upgrade mode for HTTP upgrade.

Run the **no** form of this command to switch to the automatic upgrade mode.

The default HTTP upgrade mode is manual upgrade.

Syntax

http update mode manual

no http update mode

Parameter Description

manual: Specifies the manual upgrade mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the **no http update mode** command is run to switch the HTTP upgrade mode to automatic upgrade mode, the system detects upgrade files on the server by default, automatically downloads the files, and performs an upgrade when the scheduled timer expires.

Examples

The following example configures automatic upgrade mode for HTTP upgrade.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update mode manual
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 http update server

Function

Run the **http update server** command to configure the server address and port number for HTTP upgrade.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The default server address for HTTP upgrade is **0.0.0.0** and the default port number is **80**.

Syntax

http update server { *host-name* | *ipv4-address* } [**port** *port-number* | **extend** | **uri**]

no http update server

Parameter Description

host-name: Domain name of the server.

ipv4-address: Server address.

port *port-number*: Configures the server port number. Here, *port-number* indicates the port number. The range is from 1 to 65535.

extend: Configures multiple servers.

uri: Configures URI. URI indicates the local path for storing the Web package.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The server address may not be configured because the local upgrade record file records the addresses of possible upgrade servers.
- The DNS feature needs to be enabled on the device and the DNS address needs to be configured by default.
- The server address does not support IPv6.
- During an HTTP upgrade, the device connects to the server address configured by this command. If the server address cannot be connected, the device attempts to connect to server addresses recorded in the local file in turn. If none of them are connected, the upgrade cannot be performed.

Examples

The following example sets the address of the HTTP upgrade server to 10.83.132.1 and the port number to 90.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update server 10.83.132.1 port 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 http update set oob

Function

Run the **http update set oob** command to configure HTTP upgrade using the MGMT port.

Run the **no** form of this command to configure HTTP upgrade using a common port and restore the default configuration.

The upgrade using a common port instead of a MGMT port is configured by default.

Syntax

http update set oob

no http update set oob

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is available on only the devices that support the MGMT port.

Examples

The following example configures HTTP upgrade using the MGMT port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update set oob
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 http update source_ip

Function

Run the **http update source_ip** command to configure the source IP address for HTTP upgrade.

Run the **no** form of this command to restore the default configuration, that is, no source IP address is specified.

Syntax

http update source_ip *ipv4-address*

no http update source_ip

Parameter Description

ipv4-address: IPv4 source address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a source IP address for HTTP upgrade.

Examples

The following example sets the source IP address bound for HTTP upgrade to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update source_ip 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 http update time

Function

Run the **http update time** command to configure HTTP automatic detection time.

Run the **no** form of this command to remove the configured HTTP automatic detection time and restore the default configuration.

The HTTP automatic detection time is random in the range from 00:00 to 23:59 by default.

Syntax

http update time daily *hh*:*mm*

no http update time

Parameter Description

hh:*mm*: Upgrade time, in the format of hour:minute (24-hour system). Here, *hh* indicates hours, and *mm* indicates minutes.

range *hh:mm hh:mm*: Time span for automatic upgrade.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the automatic HTTP detection time.

The device connects to the Web server as scheduled to check for available upgrade files. You can view obtained files on the Web page.

Examples

The following example sets the HTTP automatic detection time to 23:40.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update time daily 23:40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show web-server https certificate information

Function

Run the **show web-server https certificate information** command to display information about the HTTPS service certificate.

Syntax

show web-server https certificate information

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about the HTTPS service certificate.

```
Hostname> enable
Hostname# show web-server https certificate information
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 1 (0x1)
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: CN=Self-Signed-CA472E87
      Validity
         Not Before: Feb 20 07:26:51 2019 GMT
         Not After : Feb 17 07:26:51 2029 GMT
      Subject: CN=Self-Signed-CA472E87
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:ec:39:13:5a:09:da:97:d1:83:8f:a7:77:cf:b4:
               88:96:a0:85:23:68:4d:5a:c6:d3:4b:d9:c0:d6:1b:
               f4:42:29:ce:33:2e:2f:79:5e:cc:bb:bd:5f:63:5b:
               41:f3:9f:fb:82:c7:ca:8a:21:a9:c2:fb:36:db:62:
               08:3c:05:b8:a2:47:07:1a:20:99:80:24:63:a4:08:
               66:22:86:b6:aa:46:43:8a:91:7d:99:f3:8a:7c:58:
               ac:1f:ef:6c:4c:d1:d6:bf:ef:a1:77:64:4b:53:16:
```

```
                29:2f:1c:e8:ec:d6:6b:b6:34:64:32:00:1f:09:30:
                69:8d:2e:85:d5:6a:db:45:cb:b8:fd:38:ba:bd:68:
                1d:de:38:65:ef:3f:c6:90:bf:ca:1a:9e:df:c3:75:
                5f:20:bd:61:b4:bd:43:6b:77:ef:25:c6:43:0a:0f:
                dc:5a:0e:28:53:37:14:77:8b:bd:ea:14:54:c5:e1:
                45:27:c9:14:63:37:67:bc:0f:09:15:1f:73:ae:bb:
                46:b1:ad:cd:23:89:fd:2c:0c:9f:a3:34:62:f0:14:
                0d:c8:92:09:68:df:8f:69:fb:1c:49:91:d8:1c:f7:
                ee:67:a3:25:c5:9a:e2:f6:1c:a8:8c:af:7e:08:29:
                44:32:b1:d8:a9:86:04:a2:80:65:24:47:56:f4:fd:
                e4:19
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         16:b8:e2:1e:45:13:56:9c:48:ef:ec:40:fb:9a:e3:4c:da:e4:
         95:c4:3b:92:10:9a:27:a0:da:ab:45:86:4c:39:fd:73:0c:e8:
         98:8b:0e:a4:28:72:66:0a:74:cc:9c:91:71:2f:94:dd:4b:4b:
         a2:54:e5:8f:47:82:bd:82:4d:70:93:6e:af:72:ce:cf:db:e2:
         36:b1:64:1a:1f:5e:c1:d9:57:12:15:5f:81:d3:ab:40:66:2a:
         3d:ab:d4:fb:24:a6:dd:1f:82:a2:33:9d:3d:da:a7:75:fa:0d:
         e6:be:1f:3b:a9:7f:d0:94:67:bf:e7:8b:19:32:5c:ea:0f:ae:
         3e:1e:41:55:06:c9:cb:42:b9:45:de:0e:d9:48:a5:75:90:5b:
         d7:89:ff:60:f2:31:ed:d7:52:0a:3d:91:87:c3:9a:85:76:8a:
         44:6f:c5:4e:9b:65:f6:78:cf:ee:7b:28:f5:10:c8:d1:39:3f:
         13:a7:96:f1:4b:11:5f:34:96:8f:13:b1:b6:de:9c:23:9e:f6:
         9d:b8:a3:f7:03:07:76:ce:bd:f6:76:1d:fc:5d:83:1e:8e:74:
         fb:78:b6:4a:ad:73:ce:e7:71:72:7d:0a:1e:49:5d:9e:65:30:
         aa:6f:b4:2f:9d:c3:e5:e6:38:de:0b:26:20:69:98:e4:6d:99:
         d2:15:ec:bd
```

Table 1-1 Output Fields of the show web-server https certificate information Command

Field	Description
Certificate	Certificate information

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show web-server status

Function

Run the **show web-server status** command to display the configuration and status of the Web service.

Syntax

show web-server status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration and status of the Web service.

```
Hostname> enable
Hostname# show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http redirect to https: false
```

Table 1-2 Output Fields of the show web-server status Command

Field	Description
http server status	HTTP service status
http server port	HTTP service port
https server status	HTTPS service status
https server port	HTTPS service port
http redirect to https	Whether automatic HTTP redirection to HTTPS is enabled

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 webmaster level

Function

Run the **webmaster level** command to configure a username and a password for Web login and authentication.

Run the **no** form of this command to restore the default configuration.

The privilege level bound to a user is 0, username is **admin**, and plaintext password is **admin** by default.

Syntax

webmaster level *privilege-level* **username** *username* { **password** [**0** | **7**] *password* | **secret** [**0** | **8**] *secret* }

no webmaster level *privilege-level* [**username** *username*]

Parameter Description

privilege-level:-level: privilege level bound to a user.

username: Username.

0 | **7**: Specifies the encryption type of a password. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.

password: User password. Enter the ciphertext when the encryption type is **7**; otherwise, enter the plaintext.

0 | **8**: Specifies the encryption type of a password. The value **0** indicates no encryption and **8** indicates encryption using the SHA-256 algorithm. The default value is **0**.

secret: User password. Enter the SHA-256 ciphertext when the encryption type is **8**; otherwise, enter the plaintext.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After logging in to the Web server, you need to be authenticated before logging in to the Web page.
- This command is used to configure a username and a password for logging in to the Web page.

- The **no webmaster level** *privilege-level* command is run to delete all the usernames and passwords of the specified permission level.
- The **no webmaster level** *privilege-level* **username** *name* command is run to delete the specified username and password.
- Usernames and passwords involve three permission levels: Up to 10 usernames and passwords are configured for each permission level.
- The system creates account **admin** by default. The account cannot be deleted and only its password can be changed. The administrator account **admin** corresponds to the level 0 privilege. Account **admin** owns all the function privileges on the Web client and can edit other management accounts and authorize the accounts to access pages. New accounts correspond to the level 1 privilege.

Examples

The following example sets the privilege level bound to a user for logging in to the Web page to **0**, username to **Hostname**, and password to **admin**, and configures SHA-256 encryption.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# webmaster level 0 username Hostname secret admin
```

Notifications

When the default account **admin** is deleted, the following notification will be displayed:

```
%notice: Cannot cancel the default user configure!
```

When the number of configured usernames exceeds 10 at each permission level, the following notification will be displayed:

```
%notice: configure webmaster level %d server reached max 10, add failed.
```

When the configured username reaches or exceeds 32 characters, the following notification will be displayed:

```
%notice: Username too long. Please enter less than 32 characters.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 web-server http redirect-to-https

Function

Run the **web-server http redirect-to-https** command to configure automatic HTTP redirection to HTTPS.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

Automatic HTTP redirection to HTTPS is disabled by default.

Syntax

web-server http redirect-to-https

no web-server http redirect-to-https

no web-server http redirect-to-https

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- When a user uses a browser to access the Web management system through HTTP upon configuration of HTTP redirection to HTTPS, the Web server address automatically redirects to HTTPS.
- The **no web-server http redirect-to-https** or **default web-server http redirect-to-https** command is used to disable automatic HTTP redirection to HTTPS.
- HTTP automatically redirects to HTTPS only when the HTTP and HTTPS services are enabled..
- If an IP address to be accessed is a Network Address Port Translation (NAPT) address, the redirection function may fail. In this case, to access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

Examples

The following example configures HTTP redirection to HTTPS when a user accesses the Web page through HTTP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server http redirect-to-https
```

Notifications

If the HTTPS service is not enabled when HTTP redirection to HTTPS is configured, the following notification will be displayed:

```
%notice: available unless https is enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 web-server https certificate

Function

Run the **web-server https certificate** command to install an HTTPS certificate.

Run the **no** form of this command to restore the default configuration.

No HTTPS service certificate is installed by default.

Syntax

web-server https certificate { **pem** *cert-filename* **private-key** *key-filename* | **pfx** *cert-filename* } [**password** *password-text*]

no web-server https certificate

Parameter Description

pem: Imports the certificate file and private key file in the pem format.

pfx: Imports the certificate file in the pfx format from which a private key is exported.

Cert-filename:-filename: Name of the certificate file under the **flash:** drive.

Key-filename:-filename: Name of the private key file under the **flash:** drive.

password-text: Decryption password of the private key file or decryption password of the private key exported from the pfx certificate.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Run the **copy** command to copy the certificate/private key file to the **flash:** partition before running the **web-server https certificate** command to install the HTTPS service certificate. After installation, you can delete the certificate/private key file from the **flash:** partition.
- You can run the **no web-server https certificate** command to remove the installed HTTPS service certificate. After deletion, the HTTPS service will use the self-signed certificate.
- This command is not displayed in the configuration.
- After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

Examples

The following example configures the device to install the HTTP certificate: Install the certificate file **usercert.pfx** under the **flash:** partition. The password for exporting the certificate file is 123456.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server https certificate pfx usercert.pfx password 123456
```

```
*Feb 28 14:38:37: %HTTPD-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```

Notifications

When the certificate is installed, the following notification will be displayed:

```
% The certificate was successfully installed.
```

When the size of the file name exceeds 64 bytes, the following notification will be displayed:

```
% Operation failed: filename too long, should be less than 64 bytes.
```

When the certificate fails to match the private key file, the following notification will be displayed:

```
% Operation failed: certificate does not matched with private key.
```

When the certificate file does not exist or is empty, the following notification will be displayed:

```
% Operation failed: certificate file not found or is empty.
```

When the private key file does not exist or is empty, the following notification will be displayed:

```
% Operation failed: private key file not found or is empty.
```

When the password is incorrect, the following notification will be displayed:

```
% Operation failed: please input correct password.
```

When an error is reported during parsing of the certificate file or private key file, the following notification will be displayed:

```
% Operation failed: verify file failed.
```

When the certificate is not installed but the certificate deletion command is run, the following notification will be displayed:

```
% Operation failed: no certificate installed.
```

When the certificate is deleted, the following notification will be displayed:

```
% The installed certificate was successfully deleted.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 web-server https generate self-signed-certificate

Function

Run the **web-server https generate self-signed-certificate** command to generate an HTTPS service self-signed certificate again.

The HTTPS service uses the self-signed certificate by default.

Syntax

web-server https generate self-signed-certificate

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is an interactive command. After running this command, enter the information to generate a self-signed certificate as prompted including the number of RSA key modulus digits and certificate username, or press **Ctrl+C** to cancel the operation.
- If the device is installed with a third-party HTTPS service certificate, the device uses the HTTPS certificate preferentially. The re-generated self-signed certificate does not replace the current HTTPS service certificate.
- When the **show running-config** command is run, this command is not displayed.
- After the HTTPS service certificate is generated again, the browser may require you add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

Examples

The following example generates an HTTPS service self-signed certificate again.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully.
```

Notifications

When the modulus length of the entered RSA key is not in the range from 1024 to 4096 or is not a number, the following notification will be displayed:

```
% Invalid number.
```

If you press **Ctrl+C** when an input prompt is displayed, the operation will be canceled and the following notification will be displayed:

```
% Operation cancelled.
```

When the length of the entered certificate username exceeds 64 bytes, the following notification will be displayed:

```
% Input too long, should not exceed 64 bytes.
```

When a self-signed certificate is generated, the following notification will be displayed:

```
% Generate self-signed certificate successfully.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Syslog Commands

Command	Function
clear logging	Clear the logs from the memory buffer.
logging	Configure a syslog server for receiving logs.
logging buffered	Configure parameters (log severity level and buffer size) of the memory buffer for storing logs.
logging console	Configure the level of logs displayed on the console.
logging count	Enable log statistics collection.
logging delay-send file flash:	Configure the name of the log file that is buffered on the local device in the case of delayed reporting.
logging delay-send interval	Configure the interval for delayed log reporting.
logging delay-send server	Configure the IP address of the server and the reporting method for delayed log reporting.
logging delay-send terminal	Enable delayed log reporting to the console and remote terminal.
logging facility	Configure the facility value of logs.
logging file	Save logs to files. Log files can be stored in the hard disk, extended flash space, USB flash drive, or SD card.
logging file numbers	Configure the number of system log files that are written into the extended flash space.
logging flash flush	Immediately write logs in the system buffer into the flash space.
logging flash interval	Configure the interval at which you write system logs into the extended flash space.
logging filter direction	Filter the logs sent to a direction.
logging filter type	Configure the log filtering type.
logging filter rule	Configure the log filtering rule.
logging life-time level	Configure the storage time of log files in the extended flash space.

logging monitor	Configure the level of logs that are displayed in the window of the monitor terminal.
logging on	Allow the display of logs on different devices.
* MERGEFORMAT	Configure a level-based log reporting policy.
logging rate-limit	Enable logging rate limiting to limit the logs that are output per second.
logging rd on	Enable log redirection in a virtual switching unit (VSU) environment, to redirect the logs of the slave or standby device to the active device.
logging rd rate-limit	Enable log redirection rate limiting in a VSU environment to limit the logs that are redirected from the slave or standby device to the active device per second.
logging server	Configure a syslog server for receiving logs.
logging source interface	Set the source interface for log packets.
logging source ip	Configure the source IPv4 address for log packets.
logging source ipv6	Configure the source IPv6 address for log packets.
logging statistic enable	Enable periodical log reporting.
logging statistic mnemonic interval	Configure the interval of periodical log reporting.
logging statistic terminal	Enable periodical log reporting (system performance statistics logs) to the console and the remote terminal.
logging synchronous	Enable the synchronization of user input and log output to prevent interruption of user input.
logging trap	Configure the severity level of logs that are sent to the syslog server.
* MERGEFORMAT	Enable user login/logout logging.
logging userinfo command-log	Enable user operation logging.
logging performance switch	Enable performance log output.
service log-format rfc5424	Switch to the RFC5424 log format.
show logging	Display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log packets are displayed based on the timestamp from earliest to latest.

show logging config	Display the log parameter configurations and log statistics.
show logging count	Display the number of times logs are generated by each module and the last generation time.
show logging reverse	Display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.
terminal monitor	Enable log display in the window of the current monitor terminal.

1.1 clear logging

Function

Run the **clear logging** command to clear the logs from the memory buffer.

Syntax

clear logging

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

This command is used to clear log packets from the memory buffer, but cannot clear the log packet statistics.

Examples

The following example clears log packets from the memory buffer.

```
Hostname> enable
Hostname# clear logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 logging

Function

Run the **logging** command to configure a syslog server for receiving logs.

Run the **no** form of this command to remove this configuration.

Run the **no logging udp-port** command to restore the default configuration.

No syslog server is configured by default.

Syntax

logging { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot** *port-number*] [**facility** *facility-type*] [**level** *inform-level*]

no logging { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot**]

Parameter Description

ipv4-address: IPv4 address of the syslog server that receives logs.

vrf *vrf-name*: Specifies the VPN routing and forwarding table (VRF) instance connected to the syslog server. Here, *vrf-name* indicates the name of the instance.

ipv6 *ipv6-address*: Specifies the IPv6 address of the syslog server that receives logs. Here, *ipv6-address* indicates the IPv6 address of the syslog server.

udp-port *port-number*: Specifies the port number of the syslog server. Here, *port-number* indicates the port number. The range is from 1 to 65535 and the default value is **514**.

facility *facility-type*: Facility value of logs that are received by the syslog server. If the RFC5424 log format is disabled, the default facility value for logs sent to the server is **local7 (23)**. If the RFC5424 log format is enabled, such default facility value is **local0 (16)**.

level *inform-level*: Level of logs that are received by the syslog server. The value range is from 0 to 7. The default level of logs sent to the log server is information (level 6). The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a syslog server to receive logs of the device. Up to five syslog servers can be configured for a user. Logs are sent to all the configured syslog servers at the same time.

Examples

The following example configures a syslog server with IP address 10.1.1.100 and port 8099.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging ipv6 AAAA:BBBB::FFFF
```

Notifications

When more than five syslog servers are configured, the following notification will be displayed:

```
You can't configure more than 5 syslog servers!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 logging buffered

Function

Run the **logging buffered** command to configure parameters (log severity level and buffer size) of the memory buffer for storing logs.

Run the **no** form of this command to prohibit recording logs in the memory buffer.

Run the **default** form of this command to restore the default configuration.

The buffer size is 1 mega-byte and the log severity level is **7** by default.

Syntax

logging buffered [*buffer-size*] [*severity-level*]

no logging buffered

default logging buffered

Parameter Description

buffer-size: Buffer size in bytes. The value range is from 4096 to 10485760 (4 Kb to 10 Mb) and the default value is **1048576** (1 Mb).

severity-level: Log severity level. The value range is from 0 to 7. The severity level can be a level name or a digit. For details about the severity levels of logs, see Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The memory buffer space is used cyclically. If the memory buffer of specified size is fully occupied, the earliest logs are overwritten. The **show logging** command is used to display logs in the memory buffer.
- Logs in the memory buffer are stored temporarily. When the device restarts or runs the **clear logging** command, logs in the buffer are cleared. Logs should be written into the extended flash space or sent to a syslog server to track problems.
- After the system has run for a long time, modifying the log buffer size, especially a larger one, may fail, and a failure prompt will appear. The general cause is that the continuous memory space for allocation is insufficient after the system has run for a long time. You are advised to modify the log buffer size when the

system starts up.

- The logs are classified into eight levels. A smaller value indicates a higher log severity level. Logs of level 0 have the highest severity level. After the level of logs that can be displayed on the device is set, logs with a level equal to or lower than the set level will be displayed. For details, see Table 1-1.

Table 1-1 Details of Log Severity Levels

Keyword	Level	Description
Emergencies	0	Indicates that an emergency occurs and the system cannot run normally.
Alerts	1	Indicates that corrective measures must be taken immediately.
Critical	2	Indicates a critical circumstance.
Errors	3	Indicates an error message.
Warnings	4	Indicates a warning.
Notifications	5	Indicates a common but important message that requires attention.
Informational	6	Indicates an informational message.
Debugging	7	Indicates debugging information.

Examples

The following example allows only the logs of level 6 or below to be recorded in a memory buffer of 10,000 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging buffered 10000 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 logging console

Function

Run the **logging console** command to configure the level of logs displayed on the console.

Run the **no** form of this command to prohibit you from printing log packets on the console.

The default level of logs that can be displayed on the console is **7** (debugging information).

Syntax

logging console [*severity-level*]

no logging console

Parameter Description

severity-level: Severity level of log packets. The value range is from 0 to 7. Here, the severity level can be a level name or a digit. For details about the severity levels of logs, see Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After a log severity level is configured, log packets with the level equal to or lower than the configured severity level will be displayed on the console.
- The **show logging** command is used to display the log parameter configuration and relevant log statistics.

Examples

The following example sets the level of logs that can be displayed on the console to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging console informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 logging count

Function

Run the **logging count** command to enable log statistics collection.

Run the **no** form of this command to clear the log statistics and disable log statistics collection.

Log statistics collection is disabled by default.

Syntax

logging count

no logging count

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable log statistics collection. Statistics collection starts when the command is run. When the **no logging count** command is run, statistics collection is disabled and the statistics are cleared.

Examples

The following example enables log statistics collection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging count
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 logging delay-send file flash:

Function

Run the **logging delay-send file flash:** command to configure the name of the log file that is buffered on the local device in the case of delayed reporting.

Run the **no** form of this command to restore the default configuration.

The default format of the log file name is file size_device IP address_index.txt.

Syntax

logging delay-send file flash:*delay-send-filename*

no logging delay-send file

Parameter Description

delay-send-filename: Name of the log file for delayed reporting.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The configured file name cannot contain any dot (.) because the system automatically adds the index and the suffix (**.txt**) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the configured file name is **log_server**, the current file index is 5, the file size is 1000 bytes, and the IP address of the device that sends the log file is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**.
- If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is **log_server**, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address of the device sending the log file is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

Examples

The following example sets the name of the log file for delayed reporting to **log_server**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send file flash: log_server
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 logging delay-send interval

Function

Run the **logging delay-send interval** command to configure the interval for delayed log reporting.

Run the **no** form of this command to restore the default configuration.

The default interval for delayed log reporting is 3600s.

Syntax

logging delay-send interval *delay-send-interval*

no logging delay-send interval

Parameter Description

delay-send-interval: Interval for delayed log reporting in seconds. The value range is from 600 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for delayed log reporting to 600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send interval 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 logging delay-send server

Function

Run the **logging delay-send server** command to configure the IP address of the server and the reporting method for delayed log reporting.

Run the **no** form of this command to remove this configuration.

Delayed log reporting is disabled by default.

Syntax

logging delay-send server [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* | } [**vrf** *vrf-name*] [**via** *mgmt-name*] **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }**no logging delay-send server** [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**via** *mgmt-name*]

Parameter Description

oob: Indicates that the data is sent to the server through the MGMT interface of the device, that is, the data is sent to the server in the form of out-of-band communication. This parameter is available only when the device has an MGMT interface.

hostname: Domain name of the server receiving logs.

ipv-address:-address: IPv4 address of the server receiving logs.

ipv6 *ipv6-address*: Specifies the IPv6 address of the server receiving logs. *ipv6-address* indicates the IPv6 address of the server.

vrf *vrf-name*: Specifies the VPN routing and forwarding table (VRF) instance connected to the log server. *vrf-name* indicates the instance name.

via *mgmt-name*: Specifies the MGMT interface used by the syslog server when the **oob** option is included in the command.

username: Username of the FTP server.

password [**0** | **7**] *password*: Configures the password of the FTP server. **0** indicates using a plaintext password; **7** indicates using a simply encrypted ciphertext password; *password* indicates the ciphertext.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

At most five File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) servers can be configured, and each server can be configured only as the FTP server or TFTP server. Logs are simultaneously sent to all the configured FTP or TFTP servers.

Examples

The following example configures an FTP server with IP address 192.168.23.12, username of **admin**, and password of **admin**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#service log-format rfc5424
Hostname(config)# logging delay-send server 192.168.23.12 mode ftp user admin password
admin
```

The following example configures a TFTP server withIPv6 address 2000::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#service log-format rfc5424
Hostname(config)# logging delay-send server ipv6 2000::1 mode tftp
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.9 logging delay-send terminal

Function

Run the **logging delay-send terminal** command to enable delayed log reporting to the console and remote terminal.

Run the **no** form of this command to disable this feature.

Delayed log reporting to the console and remote terminal is disabled by default.

Syntax

logging delay-send terminal

no logging delay-send terminal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables delayed log reporting to the console and remote terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
Hostname(config)# logging delay-send terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 logging facility

Function

Run the **logging facility** command to configure the facility value of logs.

Run the **no** form of this command to restore the facility value to the default value (**23**).

When the RFC5424 log format is enabled, the default facility value is 16 (Local0, Local use); otherwise, the default facility value is **23** (Local7, Local use).

Syntax

logging facility *facility-type*

no logging facility

Parameter Description

facility-type: Syslog facility value. For the specific values, see *Usage Guidelines*.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The facility value of logs is used to construct the priority of logs. The calculation formula is as follows:

Priority = Facility value × 8 + Severity.

As one part of log packets, the calculated log priority is sent to the log server. The log server can be used to identify different log sources, and search and filter logs of log sources. For description of the possible facility values of Syslog, see Table 1-2.

Table 1-2 Description of Syslog Facility Values

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	Security/Authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	Security/Authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon
13 (logaudit)	Log audit
14 (logalert)	Log alert
15 (clock2)	Clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

Examples

The following example sets the facility value of syslog to **kern**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging facility kern
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 logging file

Function

Run the **logging file** command to save logs to files. Log files can be stored in the hard disk, extended flash space, USB flash drive, or SD card.

Run the **no** form of this command to remove the configuration.

Logs are not recorded in the extended flash space by default.

Syntax

logging file { **flash:***filename* **| usb0:***filename* } [*max-file-size*] [*inform-level*]

no logging file

Parameter Description

flash:: Saves log files to the extended flash drive (when there is flash2, the log files will be saved to flash2).

usb0:: Saves log files to USB0. This parameter is available only when the device has one USB port with a USB flash drive inserted. Whether this parameter is supported depends on the actual product version.

filename: Name of a log file. The name does not contain the file name extension, which is always **txt**.

max-file-size: Maximum size of a log file in bytes. The value range is from 131072 to 6291456 (128 kilobytes to 6 megabytes) and the default value is **131072** (128 kilobytes).

inform-level: Level of the logs that can be recorded in log files. The level can be a level name or a digit. The default level of logs that can be written into the extended flash space is **6**. For the levels of logs, see "Usage Guidelines".

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If there is no syslog server or logs should not be transmitted on the network for security reasons, you can save the logs to the extended flash space.
- To record the logs in extended flash space, you must purchase an extended flash disk separately. Otherwise, **logging file flash** will be automatically hidden and cannot be configured. If no FLASH2 is available, **logging file flash2** is hidden automatically and cannot be configured. Otherwise, the logs are recorded in FLASH2 after **logging file flash** is configured.
- The log file name extension is fixed to **txt**. If other types of file name extensions are configured, the system prompts a configuration failure.

Examples

The following example records the logs in the extended flash space, with the file name of **syslog.txt**, file size of 128 KB, and log level of 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging file flash:syslog
```

Notifications

If the length of a configured log file name exceeds 20 characters, for example, 21 characters, an error is prompted.

```
%Error: The file length must not be longer then 20, Current file length 21.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 logging file numbers

Function

Run the **logging file numbers** command to configure the number of system log files that are written into the extended flash space.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The default number of system log files is **16**.

Syntax

logging file numbers *file-numbers*

no logging file numbers

Parameter Description

file-numbers: Number of log files. The value range is from 2 to 16.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The system will not delete the generated log files after the number of log files is modified. Therefore, to save the extended flash space, you need to manually delete the log files generated in the system (before deletion, you can transfer the log files to an external server through TFTP). For example, 16 log files will be created by default after the function of writing logs into log files is enabled. If the device has generated 16 log files and if you want to change the number of log files to 2, new logs are overridden or overwritten in the log files with the index of 0 and 1 by turns. The existing log files with the index of 2 to 16 are retained. You can manually delete them.

Examples

The following example sets the number of log files to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging file numbers 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 logging flash flush

Function

Run the **logging flash flush** command to immediately write logs in the system buffer into the flash space.

Syntax

logging flash flush

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The **logging flash flush** command takes effect once after it configures the function above. Upon the configuration, logs in the buffer will be immediately written into the flash space.
- After the function is enabled to write logs into the flash space, the logs generated in the device will be saved in the log buffer of the system temporarily. They are not written into the flash space unless the buffer is fully occupied or the timer expires. But this command allows you to immediately write them into the flash space.

Examples

The following example immediately writes the logs in the system buffer into the flash space.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging flash flush
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (basic configuration/file system management command)

1.14 logging flash interval

Function

Run the **logging flash interval** command to configure the interval at which you write system logs into the extended flash space.

Run the **no** form of this command to remove this configuration and restore the default configuration.

Logs are written into the flash space at an interval of 3600s by default.

Syntax

logging flash interval *log-write-flash-interval*

no logging flash interval

Parameter Description

log-write-flash-interval: Interval at which you write logs into the flash space in seconds. The value range is from 1 to 51840.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent the system from writing logs into the flash space frequently, do not set the interval to a small value .

Examples

The following example sets the interval at which you write logs into the flash space to 5 min.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging flash interval 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 logging filter direction

Function

Run the **logging filter direction** command to filter the logs sent to a direction.

Run the **no** form of this command to remove this configuration.

Logs sent to all the directions are filtered by default, namely, **all** is set.

Syntax

logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

no logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter Description

all: Filters the logs sent to all the directions (including the directions of the console, virtual type terminal (VTY), log buffer, log file, and log server).

buffer: Filters the logs sent to the log buffer (the logs displayed by the **show logging** command).

file: Filters the logs sent to log files.

server: Filters the logs sent to the log server.

terminal: Filters the logs sent to the console and VTY terminal, including telnet and Secure Shell (SSH).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To filter the logs in all the directions (including the directions of the console, VTY terminal, log buffer, log file, and log server) after they match filtering rules, configure the **all** keyword.
- When you filter the logs sent to a specific direction only, for example, the filtered logs are not sent to the terminal interface but must be written into log files or sent to a log server, you only need to configure the command to filter the logs sent to the terminal.

Examples

The following example filters the logs sent to the terminal, including the console and VTY terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter direction terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 logging filter type

Function

Run the **logging filter type** command to configure the log filtering type.

Run the **no** form of this command to restore the log filtering type.

The default filtering type is **filter-only**.

Syntax

logging filter type { **contains-only** | **filter-only** }

no logging filter type

Parameter Description

contains-only: Displays only the logs that contain keywords specified in the filtering rules.

filter-only: Filters and displays the logs that contain keywords specified in the filtering rules.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Too many logs from one module may result in spamming on the terminal CLI. If you do not care about them, you can apply **filter-only** on the device to filter such logs.
- To display some logs only, you can apply **contains-only** on the device to display only the logs that match filtering rules on the terminal. Then, you can check whether any event occurs.
- If the filtering direction and filtering type instead of filtering rules are configured, the configurations do not take effect, that is, logs are not filtered.
- The **filter-only** and **contains-only** filtering types are mutually exclusive, that is, you can configure only one filtering type at a time.

Examples

The following example sets the log filtering type to **contains-only**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter type contains-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 logging filter rule

Function

Run the **logging filter rule** command to configure the log filtering rule.

Run the **no** form of this command to remove this configuration.

No log filtering rule is configured by default, that is, logs are not filtered.

Syntax

logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *inform-level* | **single-match** { **level** *inform-level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

no logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *inform-level* | **single-match** { **level** *inform-level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

Parameter Description

exact-match: Configures exact matching.

single-match: Configures single matching.

module *module-name*: Specifies the name of the module whose logs need to be filtered.

mnemonic *mnemonic-name*: Specifies the mnemonic name of the logs to be filtered.

level *inform-level*: Specifies the level of the logs to be filtered.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To filter a specific log, use the **exact-match** rule. You must specify the specific module name, mnemonic name, and log level.
- To filter some types of logs, use the **single-match** rule. You must specify the module name, log level, or mnemonic name.
- If the same module name, mnemonic name, or log level is configured in both the **single-match** and **exact-match** rules, the **single-match** rule prevails over the **exact-match** rule.

Examples

The following example sets the log filtering rule to **exact-match**, module name to **LOGIN**, log level to **5**, and mnemonic to **LOGOUT**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level
5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 logging life-time level

Function

Run the **logging life-time level** command to configure the storage time of log files in the extended flash space.

Run the **no** form of this command to remove this configuration.

No storage time is configured by default. The storage time depends on the size of the configured log files.

Syntax

logging life-time level *inform-level life-time-days*

no logging life-time level *level*

Parameter Description

inform-level: Log level. The value range is from 0 to 7.

life-time-days: Number of storage days for log files in days. The value range is from 7 to 365.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Because the sizes of extended flash space and the importance of logs at various levels are different, you are advised to configure different storage days for logs of various levels.
- When the time-based log storage function is enabled, the original log storage function based on file size becomes invalid, and the log files are stored in the **syslog/** directory of the extended flash space.

Examples

The following example sets the storage time of the logs of level 6 to 10 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging life-time level 6 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 logging monitor

Function

Run the **logging monitor** command to configure the level of logs that are displayed in the window of the monitor terminal.

Run the **no** form of this command to prohibit the window of the monitor terminal from printing log packets.

The default level of logs that are displayed in the window of the monitor terminal is **7** (debugging information).

Syntax

logging monitor [*severity-level*]

no logging monitor

Parameter Description

severity-level: Severity level of a log packet. The level can be a level name or a digit. For details about the severity levels of logs, see Table 1-1.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To display logs in the VTY window, run the **terminal monitor** command. The **logging monitor** command is used to define the level of logs that are displayed in the VTY window. For details about the severity levels of logs, see Table 1-1.

Examples

The following example sets the level of logs that are displayed in the VTY window to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging monitor informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 logging on

Function

Run the **logging on** command to allow the display of logs on different devices.

Run the **no** form of this command to disable the log display.

Logs are allowed to be displayed on different devices by default.

Syntax

logging on

no logging on

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Logs can be displayed in the console window and VTY window, or recorded in different devices, including the memory buffer, extended flash space, and syslog server. If the logging function is disabled, only the logs with a severity level lower than 1 are displayed or recorded.

Examples

The following example disables the logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no logging on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 logging policy

Function

Run the **logging policy** command to configure a level-based log reporting policy.

Run the **no** form of this command to remove a level-based log reporting policy. No level-based log reporting policy is configured by default.

Syntax

logging policy module *module-name* [**not-lesser-than**] *policy-level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

no logging policy module *module-name* [**not-lesser-than**] *policy-level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

no logging policy

Parameter Description

module-name: Module name of a level-based log reporting policy.

not-lesser-than: Configures log filtering rules for a level-based log reporting policy. When this parameter is specified, the logs of a specified level or higher are sent to the specified destination, and the other logs are filtered. When this option is not specified, the logs of a specified level or lower are sent to the specified destination, and the other logs are filtered.

policy-level: Level of logs, for which a level-based log reporting policy needs to be configured.

all: Applies the level-based log reporting policy to the logs sent in all the directions.

server: Applies the level-based log reporting policy to the logs sent to the log server only.

file: Applies the level-based log reporting policy to the logs sent to log files only.

console: Applies the level-based log reporting policy to the logs sent to the console only.

monitor: Applies the level-based log reporting policy to the logs sent to the remote terminal only.

buffer: Applies the level-based log reporting sent to the logs saved in the buffer only.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example outputs logs of level 5 or higher generated by the SYS module to the console only, but logs of level 3 or lower by the SYS module to the buffer only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging policy module SYS not-lesser-than 5 direction console
```

```
Hostname(config)# logging policy module SYS 3 direction buffer
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 logging rate-limit

Function

Run the **logging rate-limit** command to enable logging rate limiting to limit the logs that are output per second.

Run the **no** form of this command to disable the logging rate limiting.

Logging rate limiting is disabled by default.

Syntax

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** [*severity-level*]]

no logging rate-limit

Parameter Description

number: Number of logs that are processed per second. The value range is from 1 to 10000.

all: Configures rate limit for all the logs, including those of levels 0 to 7.

console: Configures the maximum number of logs that are displayed on the console per second.

except: Applies no rate limit to the logs of the specified severity level or lower. The default severity level is error (level 3), that is, no rate limit is applied to the logs of level 3 or lower.

severity-level: Severity level of logs. A smaller value indicates a higher severity level. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to prevent the output of massive logs.

Examples

The following example sets the maximum number of logs of all levels (including debugging information) that are processed per second to 10 but does not control logs of the warning level and higher.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging rate-limit all 10 except warnings
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 logging rd on

Function

Run the **logging rd on** command to enable log redirection in a virtual switching unit (VSU) environment, to redirect the logs of the slave or standby device to the active device.

Run the **no** form of this command to disable log redirection.

Log redirection is enabled by default.

Syntax

logging rd on

no logging rd on

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables log redirection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no logging rd on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 logging rd rate-limit

Function

Run the **logging rd rate-limit** command to enable log redirection rate limiting in a VSU environment to limit the logs that are redirected from the slave or standby device to the active device per second.

Run the **no** form of this command to disable log redirection rate limiting.

The log redirection limits the maximum number of logs to be redirected per second to **200** by default.

Syntax

logging rd rate-limit *number* [**except** [*severity-level*]]

no logging rd rate-limit

Parameter Description

number: Maximum number of logs that are redirected per second. The value range is from 1 to 10000.

except: Applies no rate limit to the logs of the specified severity level or lower. The default severity level is error (level 3), that is, no rate limit is applied to the logs of level 3 or lower.

severity-level: Severity level of logs. A smaller value indicates a higher severity level. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to prevent the redirection of massive logs from the slave or standby device to the active device.

Examples

The following example sets the maximum number of all logs (including debugging information) that are redirected from the slave or standby device to the active device per second to 10 but does not control logs of the warning level and higher.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging rd rate-limit 10 except warnings
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 logging server

Function

Run the **logging server** command to configure a syslog server for receiving logs.

Run the **no** form of this command to remove this configuration.

Run the **no logging server udp-port** command to restore the default configuration.

No syslog server is configured by default.

Syntax

logging server [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-prot** *port-number*] [**vrf** *vrf-name*] [**facility** *facility-type*] [**level** *inform-level*]

no logging server [**oob**] { *hostname* | *ipv4-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*]

no logging server { *hostname* | *ipv4-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*] **udp-prot**

Parameter Description

oob: Specifies out-of-band communication for the log server (sending logs to the log server through the MGMT interface). This option is available only when the device has an MGMT interface.

hostname: Domain name of the syslog server that receives logs.

ipv4-address: IPv4 address of the syslog server that receives logs.

vrf *vrf-name*: Specifies the name of the VRF instance connected to the syslog server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the syslog server that receives logs.

via *mgmt-name*: Specifies the MGMT port used by the syslog server when the **oob** option is contained in the command.

udp-port *port-number*: Specifies the port number of the syslog server. The value range is from 1 to 65535, and the default value is **514**.

facility *facility-type*: Facility value of logs that are received by the syslog server. If the RFC5424 log format is disabled, the default facility value for logs sent to the server is **local7 (23)**. If the RFC5424 log format is enabled, such default facility value is **local0 (16)**.

level *inform-level*: Level of logs that are received by the syslog server. The value range is from 0 to 7. The default level of logs sent to the log server is information (level 6). The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Up to five syslog servers are configured on one device. The logs on the device are sent to all the configured syslog servers at the same time.
- In this command, the **via** parameter is available only when the **oob** parameter is configured. But the **vrf** parameter is unavailable.
- The IPv6 server does not support **vrf** or **oob**.

Examples

The following example configures a syslog server with IP address10.1.1.100 and port 8099.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server ipv6 AAAA:BBBB::FFFF
```

Notifications

When more than five syslog servers are already configured on the device, the following notification will be displayed:

```
You can't configure more than 5 syslog servers!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 logging source interface

Function

Run the **logging source interface** command to set the source interface for log packets.

Run the **no** form of this command to remove this configuration.

No log source address is configured, and the source IP address of the log packets sent to the server is the IP address of the interface that sends the packets by default.

Syntax

logging source [**interface**] *interface-type interface-number*

no logging source [**interface**]

Parameter Description

interface-type: Interface type.

interface-number: Interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IP address of log packets sent to the syslog server is the IP address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IP address of all log packets to the IP address of an interface. Thus, the administrator can identify the device that sends the log packets based on the unique IP address. If this source interface is not configured on the device or no IP address is configured for the source interface, the source IP address of the log packets is still the IP address of the interface that sends the packets.

Examples

The following example sets the source IP address of system log packets to the address of interface Loopback 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source interface loopback 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 logging source ip

Function

Run the **logging source ip** command to configure the source IPv4 address for log packets.

Run the **no** form of this command to remove this configuration.

No source IPv4 address is configured for log packets by default.

Syntax

logging source ip *ipv4-address*

no logging source ip

Parameter Description

ipv4-address: Source IPv4 address of log packets sent to the IPv4 syslog server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IPv4 address of log packets sent to the syslog server is the IPv4 address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IPv4 address of all log packets to a fixed IPv4 address. Thus, the administrator can identify the device that sends the log packets based on the unique IPv4 address. If this IPv4 address is not configured on the device, the source IPv4 address of the log packets is still the IPv4 address of the interface that sends the packets.

Examples

The following example sets the source IP address of system log packets to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source ip 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 logging source ipv6

Function

Run the **logging source ipv6** command to configure the source IPv6 address for log packets.

Run the **no** form of this command to remove this configuration.

No source IPv6 address is configured for log packets by default.

Syntax

logging source ipv6 *ipv6-address*

no logging source ipv6

Parameter Description

ipv6-address: Source IPv6 address of log packets sent to the IPv6 syslog server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the source IPv6 address of log packets sent to the syslog server is the IPv6 address of the interface that sends the packets. To track and manage log packets, the administrator runs this command to set the source IPv6 address of all log packets to a fixed IPv6 address. Thus, the administrator can identify the device that sends the log packets based on the unique IPv6 address. If this IPv6 address is not configured on the device, the source IPv6 address of the log packets is still the IPv6 address of the interface that sends the packets.

Examples

The following example sets the source IPv6 address of system log packets to 1::1/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging source ipv6 1::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 logging statistic enable

Function

Run the **logging statistic enable** command to enable periodical log reporting.

Run the **no** form of this command to disable periodical log reporting.

Periodical log reporting is disabled by default.

Syntax

logging statistic enable

no logging statistic enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is used to enable periodical log reporting, the system outputs a series of performance statistics at an interval so that the log server can monitor the system performance.

Examples

The following example enables periodical log reporting.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 logging statistic mnemonic interval

Function

Run the **logging statistic mnemonic interval** command to configure the interval of periodical log reporting.

Run the **no** form of this command to restore the default configuration.

The interval of periodical logging is 15 min by default.

Syntax

logging statistic mnemonic *mnemonic* **interval** *logging-statistic-interval*

no logging statistic mnemonic *mnemonic*

Parameter Description

mnemonic: Mnemonic string for periodical log reporting, used to identify a statistical object of system performance.

logging-statistic-interval: Interval of periodical log reporting in minutes. The value range is 0, 15, 30, 60, and 120, where **0** indicates disabling periodical log reporting for the statistical object.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval of periodical log reporting for statistical object MATCH to 30 min.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic mnemonic MATCH interval 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 logging statistic terminal

Function

Run the **logging statistic terminal** command to enable periodical log reporting (system performance statistics logs) to the console and the remote terminal.

Run the **no** form of this command to disable this feature.

Periodical log reporting to the console and remote terminal is disabled by default.

Syntax

logging statistic terminal

no logging statistic terminal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables periodical log reporting to the console and remote terminal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging statistic terminal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 logging synchronous

Function

Run the **logging synchronous** command to enable the synchronization of user input and log output to prevent interruption of user input.

Run the **no** form of this command to disable this feature.

The synchronization of user input and log output is disabled by default.

Syntax

logging synchronous

no logging synchronous

Parameter Description

N/A

Command Modes

Line configuration mode

Default Level

14

Usage Guidelines

Run this command to enable the synchronization of user input and log output to prevent interruption of user input. If the port UP-DOWN log is displayed during input of the **configure terminal** command, the input command is output again:

```
Hostname# configure terminal
Oct  9 23:40:55 %LINK-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct  9 23:40:55 %LINEPROTO-UPDOWN: Line protocol on Interface GigabitEthernet 0/1,
changed state to DOWN
```

Examples

The following example enables the synchronization of user input and log output on the console.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# logging synchronous
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 logging trap

Function

Run the **logging trap** command to configure the severity level of logs that are sent to the syslog server.

Run the **no** form of this command to disable the function of sending log packets to the syslog server.

The default severity level of logs sent to the syslog server is **6** (informational message).

Syntax

logging trap [*severity-level*]

no logging trap

Parameter Description

severity-level: Severity level of logs. The range is from 0 to 7. The severity level can be a level name or a digit.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- To send logs to the syslog server, first configure the **logging server** command, and then use the **logging trap** command to specify the severity level of the logs to be sent. For details about the severity levels of logs, see Table 1-1.
- When the device independently configures the severity level of logs to be received by the log server, the severity level configured separately for the log server prevails.

Examples

The following example sets the severity level of logs sent to syslog server 202.101.11.22 to 6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging server 202.101.11.22
Hostname(config)# logging trap informational
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 logging userinfo

Function

Run the **logging userinfo** command to enable user login/logout logging.

Run the **no** form of this command to disable user login/logout logging.

User login/logout logging is disabled by default.

Syntax

logging userinfo

no logging userinfo

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After user login/logout logging enabled, a log will prompt the device administrator when a user connects to the device. The log format is as follows:

```
Mar 22 14:05:45 %LOGIN-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

Examples

The following example enables user login/logout logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging user-info
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 logging userinfo command-log

Function

Run the **logging userinfo command-log** command to enable user operation logging.

Run the **no** form of this command to disable user operation logging.

User operation logging is disabled by default.

Syntax

logging userinfo command-log

no logging userinfo command-log

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After user operation logging is enabled, a log will be displayed to prompt the device administrator when a user modifies device configurations. The log format is as follows:

```
Mar 22 14:10:40 %CLI-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log:
logging server 192.168.23.68.
```

- If the 5424 log format is configured using the **service log-format rfc5424** command, you need to configure the **logging delay-send terminal** command before you output the operation logs to the terminal (because delayed log reporting is registered for the operation logs).

Examples

The following example enables user operation logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging userinfo command-log
The security log has been recorded, this command does not need to be opened.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 logging performance switch

Function

Run the **logging performance switch** command to enable performance log output.

Run the **no** form of this command to disable performance log output.

Performance log output is disabled by default.

Syntax

logging performance switch

no logging performance switch

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When performance log output is enabled, the log output through the performance logging interface is transmitted through the performance log channel (that is, the logs are sent to the log server only; this mechanism usually does not need to be configured, and it is designed for the service that outputs many logs to the server rapidly).

Examples

The following example enables performance log output.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging performance switch
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 service log-format rfc5424

Function

Run the **service log-format rfc5424** command to switch to the RFC5424 log format.

Run the **no** form of this command to switch to the original log format.

The default syslog format is **RFC3164**.

Syntax

service log-format rfc5424

no service log-format rfc5424

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After the system is switched to the RFC5424 log format, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable to the original log format fail and are hidden.
- When the system is switched to the original log format, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable to the RFC5424 log format fail and are hidden.
- Before and after log format switching, the output of the **show logging** and **show logging config** commands changes.

Examples

The following example sets the log format to RFC5424.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service log-format rfc5424
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 show logging

Function

Run the **show logging** command to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log packets are displayed based on the timestamp from earliest to latest.

Syntax

show logging

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the log parameter configurations and log statistics as well as the log packets in the memory buffer when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
```

```
015487: *Sep 19 02:46:13: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to up.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to down.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to up.
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
```

Table 1-3 Output Fields of the show logging Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Standard format	Standard log format
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics collection
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Log Buffer	Log packets recorded in the memory buffer

The following example displays the log parameter configurations and log statistics as well as the log packets in the memory buffer when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
```

```
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3,
Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - Please config the IP address for
capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address for
capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - Please config the IP address for
capwap.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address for
capwap.
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
```

Table 1-4 Output Fields of the show logging Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics function
Statistic log messages	Function of periodical log reporting
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal

Field	Description
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics
Log Buffer	Log packets recorded in the memory buffer

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 show logging config

Function

Run the **show logging config** command to display the log parameter configurations and log statistics.

Syntax

show logging config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the log configurations when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
```

Table 1-5 Output Fields of the show logging config Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Standard format	Standard log format
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server as well as log statistics

The following example displays the log configurations when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
```

```
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3,
Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
```

Table 1-6 Output Fields of the show logging config Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics function
Statistic log messages	Whether to enable periodical log reporting
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 show logging count

Function

Run the **show logging count** command to display the number of times logs are generated by each module and the last generation time.

Syntax

show logging count

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the statistics on logs generated by each module in the system.

```
Hostname> enable
Hostname# show logging count
Module Name   Message Name Sev Occur     Last Time
==================================================SYS         CONFIG_I        5
1        Jul 6 10:29:57
--------------SYS      TOTAL     1
```

Table 1-7 Output Fields of the show logging count Command

Field	Description
Module Name	Log module name
Message Name	Log mnemonic name
Sev	Log level
Occur	Number of log entries of this type counted since the execution of the logging count command
Last Time	Last time that a log of this type is generated

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 show logging reverse

Function

Run the **show logging reverse** command to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.

Syntax

show logging reverse [**timestamp** *YY/MM/DD hh:mm:ss*]

Parameter Description

timestamp: Configures the timestamp, that is, the end time of the logs to be queried.

YY: Year in the timestamp.

MM: Month in the timestamp.

DD: Day in the timestamp.

hh:mm:ss: Hour, minute, and second in the timestamp.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

- This command is used to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.
- The command is also used to display the logs from the current time to the input time. The log packets are displayed based on the timestamp from latest to earliest.

Examples

The following example displays log packets based on the timestamp from latest to earliest when the RFC5424 log format is not enabled.

```
Hostname> enable
Hostname# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to up.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to down.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-UPDOWN: Line protocol on Interface
FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Hostname %LINK-UPDOWN: Interface FastEthernet 0/24, changed
state to up.
```

Table 1-8 Output Fields of the show logging reverse Command with the RFC5424 Log Format Disabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Standard format	Standard log format

Field	Description
Timestamp debug messages	Timestamp format of debugging information
Timestamp log messages	Timestamp format of logs
Sequence-number log messages	Sequence number function
Sysname log messages	Whether to enable the function of adding a system name to logs
Count log messages	Log statistics collection
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Log Buffer	Log packets recorded in the memory buffer

The following example displays log packets based on the timestamp from latest to earliest when the RFC5424 log format is enabled.

```
Hostname> enable
Hostname# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3,
Cycle:10 seconds
Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address for
capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - Please config the IP address for
capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip address for
capwap.
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - Please config the IP address for
capwap.
```

Table 1-9 Output Fields of the show logging reverse Command with the RFC5424 Log Format Enabled

Field	Description
Syslog logging	Logging function ● "enabled" is displayed when the function is enabled. ● "disabled" is displayed when the function is disabled.
Console logging	Level of the logs displayed on the console as well as log statistics
Monitor logging	Level of the logs displayed in the VTY window as well as log statistics
Buffer logging	Level of the logs recorded in the memory buffer as well as log statistics
Count log messages	Log statistics- function
Statistic log messages	Whether to enable periodical log reporting
Statistic log messages to terminal	Whether to enable periodical log reporting to the console and remote terminal
Delay-send file name	Name of the file that buffers delayed log reporting on the local device, currently written file index, and the interval of delayed log reporting
Trap logging	Level of the logs sent to the syslog server as well as log statistics
Delay-send logging	Address of the server for delayed log reporting, reporting mode, and statistics
Log Buffer	Log packets recorded in the memory buffer

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 terminal monitor

Function

Run the **terminal monitor** command to enable log display in the window of the current monitor terminal.

Run the **terminal no monitor** command to disable this feature.

Log display in the window of the current monitor terminal is disabled by default.

Syntax

terminal monitor

terminal no monitor

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is only used to configure a temporary attribute for the current VTY terminal. The temporary attribute is not stored permanently. After the VTY terminal session ends, the system will adopt the default configuration, and the temporary attribute will fail. This command is also run on the console but does not take effect.

Examples

The following example enables log display in the current VTY window.

```
Hostname> enable
Hostname# terminal monitor
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Software Upgrade Commands

Command	Function
check version	Display the version matching of each device.
show upgrade auto-sync	Display the auto-sync upgrade configuration in the device.
show upgrade file	Display information about the installation package file stored in the file system of the device.
show upgrade history	Display the upgrade history.
show upgrade status	Display the upgrade status of each board of the device and the installation status of the patch package.
upgrade	Install and upgrade the installation package in the local file system.
upgrade auto-sync package	Configure the check scope for auto-sync upgrade of the device system.
upgrade auto-sync policy	Configure an auto-sync upgrade policy for the system.
upgrade auto-sync range	Configure the auto-sync upgrade range for the system.
upgrade sync-server	Configure the auto-sync upgrade range of the system.
clear install storage	Clear all the patch packages not running currently and corresponding database information.
install add	Download a patch package and add the patch information to the database.
install activate	Activate a patch temporarily to make it take effect.
install commit	Activate a patch permanently to make the patch still effective after the device is restarted.
install deactivate	Roll back a patch to the unactivated state.
install remove	Remove an unactivated patch package and delete the patch information from the database.

install auto-sync	Enable the patch auto-sync function on the device. The configuration is valid for only newly connected devices.
show install auto-sync	Display all the patch packages that need auto-sync on the device.
show install	Display information about all the patches of the current device.
patch active	Activate the installation package of a function component.
patch running	Activate a patch permanently to make the patch still effective after the device is restarted.
patch auto-running	Activate a patch and make it take effect automatically and permanently. Namely, the patch is still effective even after the device is restarted.
patch deactive	Roll back a patch to the unactivated state.
patch delete	Remove an unactivated patch package and delete the patch information from the database.
show patch	Display information about the latest patch of the current device.
show patch detail	Display details about patches of the device.

1.1 check version

Function

Run the **check version** command to display the version matching of each device.

Syntax

check version

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the version matching of each device.

```
Hostname> enable
Hostname# check version
  Dev Slot State
  --- ---- ------------
  1   0    Compatible
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 show upgrade auto-sync

Function

Run the **show upgrade auto-sync** command to display the auto-sync upgrade configuration in the device.

Syntax

show upgrade auto-sync

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the auto-sync upgrade information of the system.

```
Hostname> enable
Hostname# show upgrade auto-sync
   auto-sync policy: coordinate
   auto-sync range:  vsu
auto-sync package: flash:/main_1.0.0.0f328e91.bin
```

Table 1-1 Output Fields of the show upgrade auto-sync Command

Field	Description
auto-sync policy	Configured auto-sync upgrade policy: ● coordinate: Synchronizes the software of all the other members to the version of the system upgrade package stored in the supervisor module. ● none: No auto-sync upgrade is performed.
auto-sync range	Range of auto-sync upgrade
auto-sync package	Path of the upgrade package for auto-sync upgrade

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 show upgrade file

Function

Run the **show upgrade file** command to display information about the installation package file stored in the file system of the device.

Syntax

show upgrade file *url*

Parameter Description

url: Local path where the installation package file is stored.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

After you download an installation package file to the local file system, you can run this command to display the main information of the installation package beforehand.

Caution

This command does not support the rack package.

Examples

The following example displays information about an installation package file.

```
Hostname> enable
Hostname# show upgrade file flash: RG-CS86_RGOS 12.6(2)B0103-FULL_install.bin
Name               : main
Version            : 1.0.0.2f1c4dd8
Package type        : unknown
Size               : 166440370
Build time          : Fri 23 Nov 2018 09:01:43 UTC
Description         : main upgrade package
Package files       :
       /fdt.img
       /initrd.img
       /kernel.img
       /rboot-CS86.bin
       /rootfs.sqsh
```

```
      /u-boot-CS86_spi.bin
```

Table 1-2 Output Fields of the show upgrade file Command

Field	Description
Name	Name of an installation package: ● main: Installation package of the main program ● bios: BIOS installation package ● cpld: Installation package for the CPLD and FPGA firmware
Version	Version of the installation package
Package type	Type of the installation package: ● distribute component: installation package for rack-type devices ● main component: Main installation package ● bios component: BIOS installation package ● cpld component: Installation package for the CPLD and FPGA firmware
Size	Size of the installation package, in bytes
Build time	Compilation time
Description	Description of the installation package
Package files	List of files in the installation package

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show upgrade history

Function

Run the **show upgrade history** command to display the upgrade history.

Syntax

show upgrade history

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the upgrade history.

```
Hostname> enable
Hostname#show upgrade history
Upgrade History Information:
       Time          : 2018-11-05 06:13:17
       Method        : OOBTFTP
       Package Name   : CS86.bin
       Package Type   : MAIN
       Time          : 2018-11-06 03:11:16
       Method        : OOBTFTP
       Package Name   : CS86_RGOS12.6(2)B0103_install.bin
       Package Type   : MAIN
```

Table 1-3 Output Fields of the show upgrade history Command

Field	Description
Upgrade History Information	Upgrade history information
Time	Upgrade time
Method	Upgrade method: ● AUTO-SYNC: Auto-sync upgrade ● LOCAL: Upgrade using the local installation package ● TFTP: Upgrade through TFTP downloading ● FTP: Upgrade through FTP downloading ● OOBTFTP: Upgrade through oob_tftp downloading ● OOBFTP: Upgrade through oob_ftp downloading
PackageName	Name of the installation package
PackageType	Type of the installation package: ● MAIN: Main installation package

Field	Description
	• RBOOT: RBOOT installation package • UBOOT: UBOOT installation package • CPLD: Installation package for the CPLD and FPGA firmware • BIOS: BIOS installation package • DISTRIBUTE: installation package for rack-type devices

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show upgrade status

Function

Run the **show upgrade status** command to display the upgrade status of each board of the device and the installation status of the patch package.

Syntax

show upgrade status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the upgrade status of each board of the device.

```
Hostname> enable
```

```
Hostname# show upgrade status
upgrade global status: INIT
[Slot 2/0]
      Device type    : CS86
      Status         : success
[Slot 1/0]
      Device type    : CS86
      Status         : success
```

The following example displays the installation status of the patch package.

```
Hostname# show upgrade status
[Slot 2/0]
      Device type    : CS86
      Status         : success
[Slot 1/0]
      Device type    : CS86
      Status         : success
```

Table 1-4 Output Fields of the show upgrade status Command

Field	Description
upgrade global status	Global status of upgrade: ● INIT: Upgrade is not performed or has been completed. ● DOWNLOAD: The downloading process of the installation package ● PRE-UPGRADE: The pre-upgrade process ● UPGRADING: The upgrading process ● POST-UPGRADE: The post-upgrade process
Device type	Device type
Status	Upgrade status of a board: ● Ready: Not upgraded ● parse: The parsing process of the installation package ● transmission: The installation package is being transmitted. ● upgrading: The installation package is being upgraded. ● success: Upgrade succeeded ● skipped: Upgrade skipped because it is not supported by the device or the version is consistent with the target version. ● fail: Upgrade failed

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 upgrade

Function

Run the **upgrade** command to install and upgrade the installation package in the local file system.

Syntax

upgrade [**boot**] { *url* | **download** { **oob_ftp:**//*path* [**via mgmt** interface-number] | **oob_tftp:**//*path* [**via mgmt** { i*nterface-number* }] | **ftp:**//*path* [**vrf** *vrf-name*] | **tftp:**//*path* [**vrf** *vrf-name*] } [**slot** *slot-number*] } [**force**]

Parameter Description

boot: Upgrades the boot on the device, including **Uboot** and **Rboot**.

url: Local path of the installation package on the device, which is **flash:**, **tmp:**, or **usb0:**. This parameter indicates that the installation package stored in the device is used for upgrade.

force: Indicates that upgrade is performed forcibly when the target upgrade version is the same as the version of the system.

path: Path of the installation package on the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server. This parameter indicates that the installation package is downloaded from the server, and then the device will upgrade itself automatically.

vrf *vrf-name*: Downloads the installation package from the specified Virtual Routing and Forwarding (VRF) table.

slot *slot-number*: Upgrades a specified board.

via mgmt *interface-number*: Specifies an MGMT interface if the installation package is transmitted through **oob_tftp** or **oob_ftp** and there are multiple MGMT interfaces. Here, *interface-number* indicates the specified MGMT interface number.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command supports installation packages of all the subsystems, installation packages of rack-type devices, and patch installation packages. Before running this command, run the **copy** command to copy the function package to the file system of the device.

The **vrf** parameter is mutually exclusive to the **oob_tftp** and **oob_ftp** parameters.

Examples

The following example sets the upgrade path of the device system to the installation package in the USB flash drive.

```
Hostname> enable
Hostname# upgrade usb0: RG-CS86_RGOS12.6(2)B0103-FULL_install.bin
< The terminal is locked by upgrade module >
Upgrade start
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!10%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!20%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!30%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!100%
Upgrade success
< The terminal is unlocked by upgrade module >
[Slot 0]
      Device type    : CS86
      Status         : success
```

The following example upgrades the patch package under the flash path in the device.

```
Hostname# upgrade flash:cmpnt_upgrade_server_99.0.0.0_mips64.deb
< The terminal is locked by patch module >
Upgrade start
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Upgrade finish
< The terminal is unlocked by patch module >
Operate result information:
-------------------------------------
Slot         Result       Comment
```

0 Success NoneNotifications

When upgrade succeeds, the following notification will be displayed:

```
Upgrade success
```

When an installation package is invalid or damaged, the following notification will be displayed. You need to obtain an installation package again and run the upgrade command.

```
Invalid package file
```

When the device does not support that installation package, the following notification will be displayed. You need to obtain the installation package again and run the upgrade command.

```
Device don't support
```

When the device does not need to be upgraded, the following notification will be displayed:

```
The version in device is newer or the same
```

When the upgrade space is insufficient, the following notification will be displayed:

```
No enough space for decompress
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show version** (basic configuration/basic management command)

1.7 upgrade auto-sync package

Function

Run the **upgrade auto-sync package** command to configure the check scope for auto-sync upgrade of the device system.

By default, the check scope for auto-sync upgrade of the system is the path of the upgrade package used in the previous system upgrade.

Syntax

upgrade auto-sync package *url*

Parameter Description

url: Local path of the used upgrade package in the device during the auto-sync upgrade of the device.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

When new members join the system, the upgrade function module determines the location of the installation package according to this path. Each time the system is upgraded, the upgrade function module automatically records the path of the installation package used for this upgrade and uses it for auto-sync upgrade. You can also run the **upgrade auto-sync package** command to manually set a path.

Examples

The following example sets the auto-sync upgrade path of the device system to the upgrade package in the USB flash drive.

```
Hostname> enable
Hostname# upgrade auto-sync package usb0:/main_1.0.0.0f328e91.bin
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show upgrade auto-sync**

1.8 upgrade auto-sync policy

Function

Run the **upgrade auto-sync policy** command to configure an auto-sync upgrade policy for the system.

The default auto-sync upgrade policy of the system is **coordinate.**

Syntax

upgrade auto-sync policy [**compatible** | **coordinate** | **none**]

Parameter Description

none: Performs no auto-sync upgrade and disables the patch package auto-sync.

compatible: Checks whether auto-sync is needed based on the sequential order of versions and enables patch package auto-sync.

coordinate: Synchronizes the version of the system upgrade package stored on the supervisor module to this version, and enables patch package auto-sync.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

Before using this command, you need to confirm whether the upgrade package is ready.

Examples

The following example configures the auto-sync upgrade policy for the device as **compatible**.

```
Hostname> enable
Hostname# upgrade auto-sync policy coordinate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show upgrade auto-sync**

1.9 upgrade auto-sync range

Function

Run the **upgrade auto-sync range** command to configure the auto-sync upgrade range for the system.

The default auto-sync upgrade range of the system is the VSU system.

Syntax

upgrade auto-sync range [**vsu**]

Parameter Description

vsu: Performs auto-sync upgrade of the version in the VSU system.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the auto-sync upgrade range to the VSU system.

```
Hostname> enable
Hostname# upgrade auto-sync range vsu
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show upgrade auto-sync**

1.10 upgrade sync-server

Function

Run the **upgrade sync-server** command to configure the auto-sync upgrade range of the system.

Syntax

upgrade sync-server [**open** | **close**]

Parameter Description

open: Enables the auto-sync service so that the version of the supervisor module is synchronized to the line card when a line card without the main program is added to the chassis.

close: Disables the auto-sync service so that the version of the supervisor module is not synchronized to the line card when a line card without the main program is added to the chassis.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

When the auto-sync upgrade range of the system is set to **open**, the line card without main program is automatically upgraded to the version consistent with the supervisor module after being inserted into the chassis in hot swap mode.

Examples

The following example enables the auto-sync service.

```
Hostname> enable
Hostname# upgrade sync-server open
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 clear install storage

This command must be used with caution, because no patch is rolled back to the previous state after this command is run.

Function

Run the **clear install storage** command to clear all the patch packages not running currently and corresponding database information.

Syntax

clear install storage [**slot** { **0 | all** }]

Parameter Description

slot-number: Slot number of a line card. It is used for rack-type devices. The value range of this parameter depends on the actual product.

0: Specifies the current device.

all: Specifies all devices.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command is used to clear all the patch packages that are not currently running, and delete the patch information from the database. After this command is run, none of the installed patches can be deactivated.

Examples

The following example clears all the patch packages from the device.

```
Hostname> enable
Hostname# clear install storage
Running this command will cause system fail to deactivate. continue?[Y/N]y
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
```

```
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example clears the patch package of the line card in slot 1/0 on the device.

```
Hostname> enable
Hostname# clear install storage slot 1/0
Running this command will cause system fail to deactivate. continue?[Y/N]y
< The terminal is lock >
Operating, please wait for a moment..
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
< The terminal is unlock >
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 install add

Function

Run the **install add** command to download a patch package and add the patch information to the database.

Syntax

install add *url* [**slot** { **0 | all** }]

Parameter Description

url: Path of downloading a patch package through **flash**, **TFTP**, **FTP**, or **HTTP**.

0: Specifies the current device.

all: Specifies all devices.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command is used to copy a patch package to the target location and add it to the database.

Examples

The following example downloads patch packages of all the versions or modules of the device and adds the patch information to the database.

```
Hostname> enable
Hostname# install add tftp//192.1.1.1/smu_rf_hot1002_0118.bin
< The terminal is lock >
Press Ctrl+C to quit
!
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example downloads a patch package to the line card in slot 1/0 on the device and adds the patch information to the database.

```
Hostname# install add tftp//192.1.1.1/smu_rf_hot1002_0118.bin slot 1/0
Press Ctrl+C to quit
!
```

```
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None

< The terminal is unlock >
```

Notifications

- After running this command, you can use the **show install** command to display the patch information. If the state is installed, the patch information is added.
- When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

  If an installed patch package is reinstalled, the following notification will be displayed:

  ```
  This package already add, don't need to add again!
  ```

  When the space for installing a patch package is insufficient, the following notification will be displayed:

  ```
  No space left on device!
  ```

  When a patch package does not match the device, the following notification will be displayed:

  ```
  Package architecture not match!
  ```

  When the device fails to meet the installation conditions of a patch package, the following notification will be displayed:

  ```
  Package depends not satisfy!
  ```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.13 install activate

Function

Run the **install activate** command to activate a patch temporarily to make it take effect.

Syntax

install activate *package_name* [**slot** { **0 | all** }]

Parameter Description

package_name: Name of the patch package file to be activated.

0: Specifies the current device.

all: Specifies all devices.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is used to activate the installation package of a function component.
- Only the installed patches can be activated.
- If an activated patch package does not take effect, the cause is that the version of each component in the current patch package is earlier than or the same as that of the component running in the current device. This is normal.
- If a patch in the device is activated but not confirmed, the patch package will be rolled back to the previous state after the device is restarted. If you confirm that the problem is solved after a patch package is activated, run the **install commit** command immediately.

Examples

The following example activates a patch temporarily to make it take effect.

```
Hostname> enable
Hostname# install activate smu_rf_hot1002_0118.bin
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
```

```
-------------------------------------
1/0          Success       None
2/0          Success       None

< The terminal is unlock >
```

The following example activates a patch for the line card in slot 1/0 temporarily to make the patch take effect.

```
Hostname# install activate smu_rf_hot1002_0118.bin slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
Slot         Result       Comment
1/0          Success       None
< The terminal is unlock >
```

Notifications

When the component package file does not exist or the device does not support the entered patch file name, the following notification will be displayed:

```
Package maybe not exist, please check!
```

When a patch package file is damaged and the verification fails, the following notification will be displayed:

```
Package verify fail, please check!
```

When the component, on which a patch package depends, is not installed, the following notification will be displayed:

```
Package depends not satisfy!
```

When the device space is insufficient, the following notification will be displayed:

```
No space left on device!
```

When a patch package error occurs, the following notification will be displayed:

```
Install package error!
```

When the patch package version is the same as or earlier than the current version of the device, the patch will not take effect and the following notification will be displayed:

```
Version is lower or same, it doesn't take effect
```

When a patch has been activated on the device, the patch will not be reactivated, the patch package will be deleted, and the following notification will be displayed:

```
All components have been activated on device, no activate again!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.14 install commit

Function

Run the **install commit** command to activate a patch permanently to make the patch still effective after the device is restarted.

Syntax

install commit [**slot** { **0 | all** }]

Parameter Description

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

- Only the active patches can be activated permanently.
- If the device is reset due to exceptions before the permanent activation, the patch automatically rolls back to its previous state.
- Only the patch packages that has been run the **install commit** command is permanently effective. Otherwise, the activated patch packages will automatically roll back to their previous states after the device is restarted.

Examples

The following example activates a patch permanently to make it still effective after the device is restarted.

```
Hostname> enable
Hostname# install commit
< The terminal is lock >
Operating, please wait for a momen
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
```

```
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
2/0           Success       None
< The terminal is unlock >
```

The following example activates the patch for the line card in slot 1/0 permanently to make the patch still effective after the device is restarted.

```
Hostname# install commit slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When there is no patch in **Active** state and you run the **install commit** command, the following notification will be displayed:

```
There are no active state on the device, no need running!
```

When no patch has been installed on the current device and you run this command, the following notification will be displayed:

```
No package in device, not need commit!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.15 install deactivate

Function

Run the **install deactivate** command to roll back a patch to the unactivated state.

Syntax

install deactivate *package_name* [**slot** { **0 | all** }]

Parameter Description

package_name: Name of a patch package file.

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example rolls back a patch to the unactivated state.

```
Hostname> enable
Hostname# install deactivate smu_rf_hot1002_0118.bin slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example rolls back the patch of the line card in slot 1/0 to the unactivated state.

```
Hostname# install deactivate smu_rf_hot1002_0118.bin slot 1/0
```

```
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
Slot          Result        Comment
1/0           Success       None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When a component package file does not exist, the device does not support the entered patch file name, or a patch package is not installed, the following notification will be displayed:

```
Package maybe not exist, please check!
```

When you deactivate an unactivated patch package, the following notification will be displayed (you need to activate a patch package before deactivating it):

```
Package is not activate or running, not allow deactivate!
```

When the device space is insufficient, the following notification will be displayed:

```
No space left on device!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.16 install remove

Function

Run the **install remove** command to remove an unactivated patch package and delete the patch information from the database.

Syntax

install remove *package_name* [**slot** { **0 | all** }]

Parameter Description

package_name: Name of a patch package file to be removed.

0: Specifies the current device.

all: Specifies all devices.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example removes an unactivated patch package from the device and deletes the patch package information from the database.

```
Hostname> enable
Hostname# install remove smu_rf_hot1002_0118.bin
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
Hostname#
```

The following example removes the unactivated patch package of the line card in slot 1/0 and deletes the patch package information from the database.

```
Hostname# install remove smu_rf_hot1002_0118.bin slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
```

```
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-----------------------------------
Slot          Result        Comment
1/0           Success       None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When you run the **install remove** command for a patch in the activated or confirmed state, the following notification will be displayed:

```
Active or running state not allow remove!
```

When you run the **install remove** command for a patch not installed, the following notification will be displayed:

```
Package is not exist, please check!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.17 install auto-sync

Function

Run the **install auto-sync** command to enable the patch auto-sync function on the device. The configuration is valid for only newly connected devices.

The patch auto-sync function is enabled by default.

Syntax

install auto-sync [**enable | disable**]

Parameter Description

enable: Enables the patch auto-sync function.

Disable: Disables the patch auto-sync function.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

You are advised to use the default configuration of the system.

Examples

The following example disables the patch auto-sync function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# install auto-sync disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show install**

1.18 show install auto-sync

Function

Run the **show install auto-sync** command to display all the patch packages that need auto-sync on the device.

Syntax

show install auto-sync

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays all the patch packages that need auto-sync on the current device.

```
Hostname> enable
Hostname# show patch auto-sync
Auto-sync switch: enable
Auto-sync lists :
    Name              State          Flag           Effective time
Package
    SP1.bin            running        Hot            1970-10-08 15:39:42     SP1
    SP2.bin            installed      Hot                                    SP2
```

Table 1-5 Output Fields of the show install auto-sync Command

Field	Description
Component auto-sync switch	Whether patch auto-sync function of a component is enabled

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show install

Function

Run the **show install** command to display information about all the patches of the current device.

Syntax

show install

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays information about all the patches of the current device.

```
Hostname> enable
Hostname# show install
Install information:
  [Slot 1/0]
    Name                    State         Flag       Effective time        Package
    smu_rf_hot1002_0118.bin    active        Hot        2019-09-17 19:00:02
    smu_rf_hot1004_0118.bin    installed     Hot        2019-09-17 19:05:01

  [Slot 2/0]
    Name                    State         Flag       Effective time        Package
    smu_rf_hot1002_0118.bin    Active        Hot        2019-09-17 19:00:02
    smu_rf_hot1004_0118.bin    install       Hot        2019-09-17 19:05:01
```

Table 1-6 Output Fields of the show install Command

Field	Description
Name	Name of a patch package
Package	Unique identifier in the patch package
State	Status of the patch package
Flag	Operation flag of the patch package
Effective time	Time when the patch package takes effect

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 patch active

Function

Run the **patch active** command to activate the installation package of a function component.

Syntax

patch active [**slot** { **0 | all** }]

Parameter Description

slot-number: Slot number of a line card. It is used for rack-type devices.

0: Specifies the current device.

all: Specifies all devices.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is used to activate the installation package of a function component. Only the installed patches can be activated.
- If an activated patch package does not take effect, the cause is that the version of each component in the current patch package is earlier than or the same as that of the component running in the current device. This is normal.
- If a patch in the device has been activated but not confirmed, the patch package will roll back to the previous state after the device is restarted. If you confirm that the problem is solved after a patch package is activated, run the **patch running** command immediately.

Examples

The following example activates the installation package of a function component in the device.

```
Hostname> enable
Hostname# patch active
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
Slot         Result       Comment
```

```
1/0          Success       None
2/0          Success       None
< The terminal is unlock >
```

Notifications

When a component package file does not exist or the device does not support the entered patch file name, the following notification will be displayed:

```
Package maybe not exist, please check!
```

When a patch package file is damaged and the verification fails, the following notification will be displayed:

```
Package verify fail, please check!
```

When the component on which a patch package depends is not installed, the following notification will be displayed:

```
Package depends not satisfy!
```

When the device space is not sufficient, the following notification will be displayed:

```
No space left on device!
```

When an activated patch package is reactivated, the following notification will be displayed:

```
Package has been activated, no need activate again!
```

When a patch package error occurs, the following notification will be displayed:

```
Install package error!
```

When the patch package version is the same as or earlier than the version of the device and fails to take effect, the following notification will be displayed:

```
Version is lower or same, it doesn't take effect
```

An activated patch on the device will not be reactivated, this patch package will be deleted, and the following notification will be displayed:

```
All components have been activated on device, no activate again!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show patch**

1.21 patch running

Function

Run the **patch running** command to activate a patch permanently to make the patch still effective after the device is restarted.

Syntax

patch running [**slot** { **0 | all** }]

Parameter Description

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

- Only the active patches can be activated permanently.
- If the device is reset due to exceptions when a patch is not in the permanently activated state, the patch automatically rolls back to the previous state.
- Only a patch package that has been run the **patch running** command is permanently effective. Otherwise, the activated patch package will automatically roll back to the previous state after the device is restarted.

Examples

The following example activates a patch permanently to make it still effective after the device is restarted.

```
Hostname> enable
Hostname# patch running
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example permanently activates the patch of the line card in slot 1/0 to make it still effective after the device is restarted.

```
Hostname> enable
Hostname# patch running slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
```

```
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When there is no patch in **Active** state and you run the **install commit** command, the following notification will be displayed:

```
There are no active state on the device, no need running!
```

When no patch has been installed on the current device and you run this command, the following notification will be displayed:

```
No package in device, not need commit!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show patch**

1.22 patch auto-running

Function

Run the **patch auto-running** command to activate a patch and make it take effect automatically and permanently. Namely, the patch is still effective even after the device is restarted**.**

Syntax

patch auto-running [**slot** { **0 | all** }]

Parameter Description

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

- You can run this command for the patches to be activated only.
- After this command is run and the configuration is confirmed to take effect, the patch will not roll back to the previous state even if the device is restarted.

Examples

The following example activates a patch and makes it permanently effective.

```
Hostname> enable
Hostname# patch auto-running
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example activates the patch of the line card in slot 1/0 and makes it permanently effective.

```
Hostname> enable
Hostname# patch auto-running slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
```

```
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When there is no patch in **Active** state and you run the **install commit** command, the following notification will be displayed:

```
There are no active state on the device, no need running!
```

When no patch has been installed on the current device and you run this command, the following notification will be displayed:

```
No package in device, not need commit!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show patch**

1.23 patch deactive

Function

Run the **patch deactive** command to roll back a patch to the unactivated state.

Syntax

patch deactive [**slot** { **0 | all** }]

Parameter Description

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

When no parameter is set in this command, it is used to delete unactivated patch packages and database information of all the device members from the device.

Examples

The following example rolls back a patch to the unactivated state.

```
Hostname> enable
```

```
Hostname# patch deactive
< The terminal is lock >
Hostname> enable
Hostname# patch auto-running
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
Patch operation finish!
Operate result information:
-------------------------------------
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example rolls back the patch of the line card in slot 1/0 to the unactivated state.

```
Hostname> enable
Hostname# patch deactive slot 1/0
< The terminal is lock >
Hostname> enable
Hostname# patch auto-running
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
```

```
< The terminal is unlock >
Patch operation finish!
Operate result information:
-----------------------------------
1/0          Success       None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When a component package file does not exist, the device does not support the entered patch file name, or a patch package is not installed, the following notification will be displayed:

```
Package maybe not exist, please check!
```

When you deactivate an unactivated patch package, the following notification will be displayed (you need to activate a patch package before deactivating it):

```
Package is not activate or running, not allow deactivate!
```

When the device space is insufficient, the following notification will be displayed:

```
No space left on device!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show patch**

1.24 patch delete

Function

Run the **patch delete** command to remove an unactivated patch package and delete the patch information from the database.

Syntax

patch delete [**slot** { **0 | all** }]

Parameter Description

0: Specifies the current device.

all**: Specifies all devices. Command Modes**

Privileged EXEC mode

Default Level

15

Usage Guidelines

When no parameter is set in this command, it is used to delete unactivated patch packages and database information of all the device members from the device.

Examples

The following example removes unactivated patch packages and deletes the patch information from database.

```
Hostname> enable
Hostname# patch delete
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None
< The terminal is unlock >
```

The following example removes the unactivated patch package of the line card in slot 1/0 and deletes the patch information from the database.

```
Hostname> enable
Hostname# patch delete slot 1/0
< The terminal is lock >
Operating, please wait for a moment
!!!!!!!!!!  20%
!!!!!!!!!!  40%
!!!!!!!!!!  60%
!!!!!!!!!!  80%
!!!!!!!!!!  90%
!!!!!!!!!!  90%
!!       100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
< The terminal is unlock >
```

Notifications

When an error is reported during running of the command, the format is the same as that in the above guidelines, and the result is **Fail** or **Skip**. The comments are described as follows:

When you run the **patch delete** command for a patch in the activated or confirmed state, the following notification will be displayed:

```
Active or running state not allow remove!
```

When you run the **patch delete** command for a patch not installed, the following notification will be displayed:

```
Package is not exist, please check!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show patch**

1.25 show patch

Function

Run the **show patch** command to display information about the latest patch of the current device.

Syntax

show patch

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays information about the latest patch of the current device.

```
Hostname# show patch
  [Slot 1/0]:
     Patch package SP1 installed in the system, version:5.0.0.0
    ----------------------------------------
    Patch      : SP1.bin
```

```
  Status     : active
  Version    : 5.0.0.0
  Size       : 1770
  Install time: 2020-07-06 06:59:28
  Description : test SP1


[Slot 2/0]:
   Patch package SP1 installed in the system, version:5.0.0.0
  ----------------------------------------
  Patch      : SP1.bin
  Status     : active
  Version    : 5.0.0.0
  Size       : 1770
  Install time: 2020-07-06 06:59:28
  Description : test SP1
```

Table 1-7 Output Fields of the show patch Command

Field	Description
Patch	Name of a patch package
Status	Status of the patch package
Version	Version of the patch package
Size	Size of the patch package
Install time	Time when the patch package takes effect
Description	Description of the patch package

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show patch detail

Function

Run the **show patch detail** command to display details about patches of the device.

Syntax

show patch detail

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays details about patches of the device.

```
Hostname# show patch detail
  [Slot 1/0]:
    Patch package SP4 installed in the system, version:5.0.0.4
    ----------------------------------------
    Patch      : SP4.bin
    Status     : active
    Version    : 5.0.0.4
    Size       : 5248
    Install time: 1970-05-29 15:43:27
    Description : test SP4
    Flag       : Hot
    Last patch  : SP1
Include    : rf_test6; rf_test7; rf_test8; rf_test5;
```

Table 1-8 Output Fields of the show patch detail Command

Field	Description
Patch	Name of a patch package
Version	Version of the patch package
Size	Size of the patch package
Install time	Activation time of the patch package

Field	Description
Description	Description of the patch package
Flag	Whether the patch is a hot patch or cold patch ● Hot: Hot patch ● Cold: Cold patch
Last patch	Name of the patch package of the last version
Include	Files included in the patch package

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Time Range Commands

Command	Function
absolute	Configure an absolute time range.
periodic	Configure a period.
show time-range	Display information about a time range.
time-range	Create a time range and enter the time range configuration mode.

1.1 absolute

Function

Run the **absolute** command to configure an absolute time range.

Run the **no** form of this command to delete an existing absolute time range.

No absolute time range is configured by default. In this case, the maximum time range is used.

Syntax

absolute { **start** *hh:mm DD/MM/YY* | **end** *hh:mm DD/MM/YY* } *

no absolute

Parameter Description

start *hh:mm DD/MM/YY*: Configures the start time of a time range. Here, *hh* indicates the hour, *mm* indicates the minute, *DD* indicates the day, *MM* indicates the month, and *YY* indicates the year.

end *hh:mm DD/MM/YY*: Configures the end time of a time range. Here, *hh* indicates the hour, *mm* indicates the minute, *DD* indicates the day, *MM* indicates the month, and *YY* indicates the year.

Command Modes

Time range configuration mode

Default Level

14

Usage Guidelines

To enable a function in an absolute time range, run the **absolute** command to configure a time range that includes start time and end time.

Examples

The following example configures a time range named **no-http** and configures an absolute time range from 00:00 on January 1, 2013 to 23:59 on December 31, 2014 in time range configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# time-range no-http
Hostname(config-time-range)# absolute start 0:0 1 Jan 2013 end 23:59 31 Dec 2014
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show time-range**

1.2 periodic

Function

Run the **periodic** command to configure a period.

Run the **no** form of this command to delete an existing period.

No period is configured by default. The current time is considered to be within a period.

Syntax

periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

no periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

Parameter Description

day-of-the-week: Day when a period starts or ends in a week.

time: Time when a period starts or ends.

Command Modes

Time range configuration mode

Default Level

14

Usage Guidelines

- To enable a function in a period, run the **periodic** command to configure a period.
- Before modifying a period for a service, you are advised to disassociate the time range. After the period is modified, associate the time range again.

Examples

The following example configures a time range named **no-http** and configures a period from Monday 01:01 to Tuesday 02:02 in time range configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# time-range no-http
Hostname(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show time-range

1.3 show time-range

Function

Run the **show time-range** command to display information about a time range.

Syntax

show time-range [*time-range-name*]

Parameter Description

time-range-name: Specified information about a time range.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about a time range.

```
Hostname> enable
Hostname# show time-range
time-range entry: test (active)
  absolute end 01:02 02 February 2012
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 time-range

Function

Run the **time-range** command to create a time range and enter the time range configuration mode.

Run the **no** form of this command to delete an existing time range.

No time range is configured by default.

Syntax

time-range *time-range-name*

no time-range *time-range-name*

Parameter Description

time-range-name: Name of a time range to be created.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When some services run based on time, for example, to make an access control list (ACL) take effect only on Monday, first create a time range and then configure Monday for time control in time range configuration mode.

Examples

The following example configures a time range named **no-http**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show time-range**

1 Supervisor Module Redundancy Commands

Command	Function
auto-sync time-period	Configure an interval for automatically synchronizing configuration files in case of redundancy of dual supervisor modules or a VSU consisting of box-type devices deployed in stacking mode.
redundancy	Enter the redundancy configuration mode.
redundancy forceswitch	Perform master/slave switchover manually.
redundancy reload	Reset a device.
show redundancy states	Display the redundancy status of the current device.

1.1 auto-sync time-period

Function

Run the **auto-sync time-period** command to configure an interval for automatically synchronizing configuration files in case of redundancy of dual supervisor modules or a VSU consisting of box-type devices deployed in stacking mode.

Run the **no** form of this command to disable automatic synchronization of such dual supervisor modules or a VSU.

Run the **default** form of this command to restore the interval for automatically synchronizing configuration files to the default value.

Automatic synchronization is enabled by default, the **startup-config** and **running-config** files are automatically synchronized, and the automatic synchronization interval is 1 hour.

Syntax

auto-sync time-period *synchronization-interval-time*

no auto-sync time-period

default auto-sync time-period

Parameter Description

synchronization-interval-time: Automatic synchronization interval, in seconds. The value range is from 1 to 2678400.

Command Modes

Redundancy configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the automatic synchronization interval to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# redundancy
Hostname(config-red)# auto-sync time-period 60
Redundancy auto-sync time-period: enabled (60 seconds).
Hostname(config-red)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show redundancy states**

1.2 redundancy

Function

Run the **redundancy** command to enter the redundancy configuration mode.

Syntax

redundancy

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enters the redundancy configuration mode.

```
Hostname> enable
Hostname# config terminal
Hostname(config)# redundancy
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 redundancy forceswitch

Function

Run the **redundancy forceswitch** command to perform master/slave switchover manually.

Syntax

redundancy forceswitch

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When this command is run on the master device, the master device is reset and the slave device becomes the new master device.

The following conditions must be met for the hot-backup switchover:

- The operation is performed on the master device and a slave device exists.
- The hot backup of all VSDs in the system is in the real-time state.
- The hot-backup switchover of all VSDs in the system is not temporarily disabled by service entities.
- When this command is run, the system with multiple VSDs determines whether each VSD allows master/slave switchover in the hot backup state. If a VSD does not allow such switchover, this command is not run; otherwise, such switchover is forcibly performed on all VSDs in the hot backup state.

Examples

The following example configures the device to switch over between the master and slave devices.

```
Hostname> enable
Hostname# redundancy forceswitch
This operation will reload the master unit and force switchover to the slave unit.
Are you sure to continue? [N/y] y
```

Notifications

When the slave device does not exist during switchover, the following notification will be displayed:

```
% Redundancy Switchover Request can only take effect while peer Supervisor is Ready.
```

When batch hot backup between the master device and the slave device in a VSD is not switched over, the following notification will be displayed:

```
% Redundancy Switchover failed: Some VSD's redundancy state is temporarily
non-realtime.
```

When the master/slave switchover of a VSD is disabled during switchover, the following notification will be displayed:

```
% Redundancy Switchover failed: Some VSD's redundancy switchover is temporarily
disabled by elements.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 redundancy reload

Function

Run the **redundancy reload** command to reset a device.

Syntax

redundancy reload { **peer** | **shelf** [*switch-id*] }

Parameter Description

peer: Resets only the slave device.

shelf: Resets both the master and slave devices in standalone mode. In VSU mode, the ID of the device to be reset must be specified.

switch-id: ID of a device in a VSU. This parameter supports VSU mode.

Note

This parameter does not support standalone mode. In VSU mode, you must enter it in the **redundancy reload shelf** command.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

- In standalone mode, the command for resetting a device is **redundancy reload shelf**, that is, the whole device is reset.
- In VSU mode, the command for resetting a device is **redundancy reload shelf** *switchid*, that is, the device with a specified device ID is reset.
  - If the master device is reset and the hot backup of the system is not real-time, the whole VSU system is reset.
  - If only the slave device is reset, data forwarding is not affected. During the resetting of the slave device,

data forwarding is not interrupted or user session information is not lost.

Examples

The following example resets device 2 in VSU mode.

```
Hostname> enable
Hostname# redundancy reload shelf 2
This operation will reload the device 2. Are you sure to continue? [N/y] y
Preparing to reload device 2!
```

Notifications

When only one device exists, the following notification will be displayed:

```
% Privileged command reload peer can only execute in Duplex Supervisor mode.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show redundancy states

Function

Run the **show redundancy states** command to display the redundancy status of the current device.

Syntax

show redundancy states

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

- Only 1:1 hot backup is supported (hot backup for the global master device and global slave device) in VSU mode. Other devices are used as candidate devices and do not participate in hot backup.
- If other VSDs are configured in the system, the hot backup status of other VSDs is displayed under VSD 0 of the global master and slave devices.

Examples

The following example displays the redundancy status of the current master device.

```
Hostname> enable
Hostname# show redundancy states
Redundancy switching function: enabled
Redundancy role: master
Redundancy state: realtime
Auto-sync time-period: 3600 s
Redundancy management role: master
Redundancy control role: active
Redundancy control state: realtime
Auto-sync time-period: 3600 s
```

The following example displays the redundancy status of the current slave device.

```
Hostname-STANDBY > enable
Hostname-STANDBY# show redundancy states
Redundancy role: slave
Redundancy state: realtime
Redundancy management role: slave
Redundancy control role: standby
Redundancy control state: realtime
Data backup state: NA
```

The following example displays the redundancy status of the current candidate device.

```
Hostname-Candidate > enable
Hostname-Candidate # show redundancy states
Redundancy role: candidate
Redundancy state: none
Redundancy management role: candidate
Redundancy control role: standby
Redundancy control state: realtime
```

The following example displays the redundancy status of the current master device when VSD1 and VSD2 are configured.

```
Hostname> enable
Hostname# show redundancy states
Redundancy switching function: enabled
Redundancy role: master
Redundancy state: realtime
Auto-sync time-period: 3600 s
Redundancy management role: master
Redundancy control role: active
Redundancy control state: realtime
Auto-sync time-period: 3600 s
VSD vsd1 redundancy state: realtime
VSD vsd2 redundancy state: realtime
```

Table 1-1 Output Fields of the show redundancy states Command

Field	Description
role	Role of a device
state	Status of the device
Auto-sync time-period	Interval for automatically synchronizing configuration files, which is displayed on only the master device. If **disabled** is displayed, automatic synchronization is disabled.
VSD <vsd name> redundancy state	Hot backup state of a VSD, which is displayed under only VSD 0 of the master and slave devices.
Redundancy switching function	Function of forcible redundancy switching of the device. If **enabled** is displayed, the function is enabled; if **disabled** is displayed, the function is disabled.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Hot Swapping Commands

Command	Function
sysmac	Specify a MAC address for the system.
remove configuration device	Remove the existing configurations of a VSU member device (this command is available only in VSU mode, and this operation takes effect after the device is restarted).
show alarm	Display current system-level alarms.
show manuinfo	Display the asset information of all independent components in the current system.
show sysmac	Display the current system MAC address of a device.
show version module detail	Display the details of a module.
show version slots	Display the online status of a module.

1.1 sysmac

Function

Run the **sysmac** command to specify a MAC address for the system.

Run the **no** form of this command to delete the MAC address retained in the configuration file.

No MAC address is specified for the system by default.

Syntax

sysmac *mac-address*

no sysmac

Parameter Description

mac-address: MAC address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Generally, the MAC address used by the system is stored in the supervisor module or flash memory of the chassis. In virtual switching unit (VSU) mode, however, the system automatically saves the used MAC address in the configuration file to avoid interruption caused by the change of the MAC address. If a valid MAC address exists in the configuration file after restart, the MAC address is used preferentially. The **no sysmac** command is run to delete the MAC address in the configuration file and restore the MAC address that is stored in the flash memory by default.

In gateway mode (the **auth-mode gateway** command is configured in the system), the gateway MAC address is bound on some peripheral devices. If the gateway is replaced, users can run the **sysmac** command to set the MAC address of the gateway to the MAC address of the new gateway. Thus, you do not need to modify configurations of downstream devices with the gateway MAC address bound. The **sysmac** command is available only when the system is configured to work in gateway mode.

After an MAC address is specified for the system or the MAC address stored in the configuration file is deleted, be sure to save the configurations and restart the system so that the configurations take effect.

The **sysmac** command is available only when the system is configured to work in gateway mode. In other modes, this command is visible but not configurable.

Examples

The following example deletes the MAC address stored in the configuration file.

```
Hostname> enable
Hostname# no sysmac
```

The following example sets the MAC address of the system to 00d0.f822.33e2.

```
Hostname> enable
```

```
Hostname# sysmac 00d0.f822.33e2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 remove configuration device

Function

Run the **remove configuration device** command to remove the existing configurations of a VSU member device (this command is available only in VSU mode, and this operation takes effect after the device is restarted).

Syntax

remove configuration device *device-id*

Parameter Description

device-id: Chassis ID.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To remove the existing configurations of a member device in the VSU system, run this command. This command is saved, and then takes effect after the system is restarted.

Examples

The following example removes the configurations of device 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# remove configuration device 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 show alarm

Function

Run the **show alarm** command to display current system-level alarms.

Syntax

show alarm

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to display current system-level alarms, including board startup failure, device temperature, power supply, fan, and inter-board data forwarding path.

Examples

N/A

Notifications

When this command is run to display current system-level alarms, the following notification will be displayed:

```
Hostname> enable
Hostname# show alarm
Dev  Module         Level    Info
1    DEV           Warning  Some fans are absent.
1    DEV           Critical Some cards are in cannot-startup state.
```

Table 1-1 Output Fields of the show alarm Command

Field	Description
Dev	ID of a device giving an alarm

Field	Description
Module	Name of the service module that reports the alarm
Level	Alarm levels, including **Critical** and **Warning**
Info	Description of the alarm causes, for example, the system power is insufficient, the fan is removed, or a board cannot be started.

Platform Description

N/A

Related Commands

N/A

1.4 show manuinfo

Function

Run the **show manuinfo** command to display the asset information of all independent components in the current system.

Syntax

show manuinfo

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the asset information of all independent components in the system for asset management. The components include the chassis, fans, power supply, supervisor modules, and line cards. The displayed information about each component includes the number, slot ID, name, serial number, software and hardware versions, and MAC address. Different information is displayed for each type of device, and only the actually supported information is displayed.

Examples

The following example displays asset information in standalone mode.

```
Hostname> enable
Hostname# show manuinfo
Device 1
   Location:                Chassis
```

```
   Device name:              RG S12006
   Device Serial Number:       62150129A8B0DAF0F0321
   Hardware Version:          V1.0
   Mac Address:              00.D0.F8.00.11.22
Device 2
   Location:                 Slot-M1
   Device name:              M12000 CM
   Device Serial Number:       32150129A8B0DAF0F0321
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
   Mac Address:              00.D0.F8.00.11.34
Device 3
   Location:                 Slot-1
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0322
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 4
   Location:                 Slot-2
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0323
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 5
   Location:                 Power 1
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0321
   Hardware Version:          V1.0
Device 6
   Location:                 Power 2
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0322
   Hardware Version:          V1.0
Device 7
   Location:                 FAN
   Device name:              M12000 FAN
   Device Serial Number:       52150129A8B0DAF0F0321
   Hardware Version:          V1.0
```

The following example displays asset information in VSU mode.

```
Hostname> enable
Hostname# show manuinfo
Device 1
   Location:                 Chassis 1
   Device name:              RG S12006
   Device Serial Number:       62150129A8B0DAF0F0321
   Hardware Version:          V1.0
```

```
   Mac Address:              00.D0.F8.00.11.22
Device 2
   Location:                 Slot-1/M1
   Device name:              M12000 CM
   Device Serial Number:       32150129A8B0DAF0F0321
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
   Mac Address:              00.D0.F8.00.11.56
Device 3
   Location:                 Slot-1/1
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0322
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 4
   Location:                 Slot-1/2
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0323
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 5
   Location:                 Power 1/1
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0321
   Hardware Version:          V1.0
Device 6
   Location:                 Power 1/2
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0322
   Hardware Version:          V1.0
Device 7
   Location:                 FAN 1
   Device name:              M12000 FAN
   Device Serial Number:       52150129A8B0DAF0F0322
   Hardware Version:          V1.0
Device 8
   Location:                 Chassis 2
   Device name:              RG S12006
   Device Serial Number:       62150129A8B0DAF0F0322
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
   Mac Address:              00.D0.F8.00.11.33
Device 9
   Location:                 Slot-2/M1
   Device name:              M12000 CM
   Device Serial Number:       32150129A8B0DAF0F0324
```

```
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
   Mac Address:              00.D0.F8.00.11.22
Device 10
   Location:                 Slot-2/1
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0325
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 11
   Location:                 Slot-2/2
   Device name:              M12000-04XFP-EA
   Device Serial Number:       32150129A8B0DAF0F0326
   Hardware Version:          V1.0
   Software Version:          RGOS 10.4(3b17) Release 129646
Device 12
   Location:                 Power 2/1
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0323
   Hardware Version:          V1.0
Device 13
   Location:                 Power 2/2
   Device name:              RG PD1200I
   Device Serial Number:       42150129A8B0DAF0F0324
   Hardware Version:          V1.0
Device 14
   Location:                 FAN 2
   Device name:              M12000 FAN
   Device Serial Number:       52150129A8B0DAF0F0322
   Hardware Version:          V1.0
```

Table 1-2 Output Fields of the show manuinfo Command

Field	Description
Location	Location of a device in the system
Device name	Device name
Device Serial Number	Device SN
Hardware Version	Hardware version

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show sysmac

Function

Run the **show sysmac** command to display the current system MAC address of a device.

Syntax

show sysmac

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the current MAC address of the system.

Examples

The following example displays the current MAC address of the system.

```
Hostname# enable
Hostname# show sysmac
00d0.f822.33e2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show version module detail

Function

Run the **show version module detail** command to display the details of a module.

Syntax

show version module detail [*slot-num*]

show version module detail [*device-id / slot-num*]

Parameter Description

device-id: Chassis ID. This parameter is optional (in VSU mode, to enter a slot ID, you must also enter the chassis ID of the module).

slot-num: Slot ID (optional).

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the details of a module.

Examples

The following example displays the details of the module in slot 0.

```
Hostname# enable
Hostname# show version module detail 2
Device  : 1
Slot    : 0
Soft Status:  master
Online Module
Type    :
Ports   : 0
Hardware version :
Software version :
BOOT version     :
Serial number    :
```

Table 1-3 Output Fields of the show version module detail 2 Command

Field	Description
Device	Device ID
Slot	Slot ID
Soft Status	Software status
Online Module	Online module
Type	Type
Ports	Number of ports
Hardware version	Hardware version
Software version	Software version
BOOT version	Boot version

Field	Description
Serial number	Serial number

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show version slots

Function

Run the **show version slots** command to display the online status of a module.

Syntax

show version slots [*slot-num*]

show version slots [*device-id* / *slot-num*]

Parameter Description

device-id: Chassis ID. This parameter is optional (in VSU mode, to enter a slot ID, you must also enter the chassis ID of the module).

slot-num: Slot ID (optional).

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the online status of a module.

Examples

The following example displays the online status of a module.

```
Hostname# enable
Hostname# show version slots
Dev  Slot  Port Configured Module   Online Module    Software Status
-  --  --------   ---           -----
1    1     0    none             none              none
1    2     24   M8606-24SFP/12GT   M8606-24SFP/12GT    none
```

```
1    3     2     M8606-2XFP         M8606-2XFP          cannot startup
1    4     24    M8606-24GT/12SFP   M8606-24GT/12SFP    ok
1    M1    0     N/A              M8606-CM           master
1    M2    0     N/A             none                none
```

Table 1-4 Output Fields of the show version slots Command

Field	Description
Dev	Device ID
Slot	Slot ID
Port	Number of ports
Configured Module	Configured module
Online Module	Online module
Software Status	Software status

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 Process Restarting Commands

Command	Function
cmdk restart	Restart a specified process of the board in a specified slot on a specified device.
cmdk start	Start a specified process of the board in a specified slot on a specified device.
cmdk stop	Stop a specified process of the board in a specified slot on a specified device.
cmdk detail	Display the process of the board in a specified slot on a specified device.
debug cmdk	Enable or disable the CMDK debugging mode.

1.1 cmdk restart

Function

Run the **cmdk restart** command to restart a specified process of the board in a specified slot on a specified device.

Syntax

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **restart**

Parameter Description

device-id: Device ID. The default value is **1**.

slot-id: Slot ID of a board.

module-name: Module name.

Table 1-1 Definitions of Slot IDs in the Command String

Slot	Slot ID
Supervisor Module 1	M1
Supervisor Module 2	M2
Interface board	Slot ID corresponding to the interface board. The value range is from 1 to 8.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is run on only the master device.
- You can run the **show version slot** command to query the device ID and slot ID of a board.

Examples

The following example restarts the span process of the board in slot 0 on device 1.

```
Hostname> enable
Hostname# cmdk device 1 slot 0 module span restart
Hostname# This operation will reset the span. Are you sure to continue? [N/y]y
```

Notifications

For the names of modules that can be restarted, see Table 1-2.

Table 1-2 Names of Modules That Can Be Restarted

Module Name	Description
aaad	Function of the AAA service
acld	Function of the ACL service
aclk	Kernel function of the ACL service
bfd	Function of the BFD service
bgp	Function of the BGP service
bridge	Function of the bridge service
ce.cap.sw	Capability framework
ce.cli.cpp.dp	CPP CLI function
ce.cpp.dp	Unified data plane of CPP
ce.ddos.sw	Defense against DDoS attacks
ce.ebrg.dp	Virtual bridge management
ce.emac.dp	Unified MAC data plane
ce.fp.sw	Basic policy service
ce.l2ofd.sw	Monitoring whether L2 user traffic is online
ce.mmu.dp	Data plane maintenance of MMU supervisor module
ce.nacm.sw	Access control management
ce.ofdpa.sw	OpenFlow data plane adaptation
ce.proxy.brg.dp	Bridge agent module
ce.proxy.traf	Traffic agent module
ce.qinq.dp	Data plane maintenance of QinQ Supervisor Module
ce.qos.sw	Data plane maintenance of QoS Supervisor Module
ce.tran.cap.sw	Cards notifying that the DM capability is ready (related to pre-installation)
ce.virvlan.dp	VLAN management
ce_ap	AP aggregation port service
ce_dad	DAD dual active device detection
ce_ddm	Data plane management of switching equipment
ce_efm	Express forwarding management

Module Name	Description
ce_lspan	Local mirror
ce_mgmt	MGMT port service maintenance
ce_mlag	Data plane service of MLAG
ce_ptm_core	Port management core module
ce_ptm_mib	Port management MIB processing module
ce_ptm_split	Port management split port
ce_ptm_trnscr	Supervisor module interface plug-in management
ce_sflow	Traffic sampling function
cli-proxy	Function of the CLI configuration agent service
cli-server	Function of the CLI configuration service
dhcp6c	Function of the DHCPv6 client service
dhcpc	Function of the DHCP client service
dm_app_pd	Device management framework
dm_dp	Device management core protocol
dm_kernel_sw	Device management kernel module - switching product
dns_client	Function of the DNS client service
efmp_frame	Function of the fast forwarding service
efmp_proxy	Function of the fast forwarding agent service
fe.cap.sw	Line card capability framework
fe.cpp.sw	Line card CPP module
fe.ebrg.sw	Line card virtual bridge
fe.emac.sw	Line card MAC management
fe.fp.sw	FP security entry maintenance service
fe.mmu.sw	MMU cache management service
fe.ofdpa.sw	Line card OpenFlow data plane module
fe.qinq.sw	QinQ data plane service
fe.qos.sw	QoS data plane service
fe.virvlan.sw	VLAN data plane service

Module Name	Description
fe_ap	Line card aggregation port management module
fe_bfd	BFD service
fe_dad	DAD dual active device detection service
fe_ddm	Device management module on the line card data plane
fe_efm	Line card express forwarding
fe_mlag	Forwarding plane service of MLAG
fe_ptm_core	Interface management core service
fe_ptm_mib	Interface MIB service
fe_ptm_split	Interface splitting service
fe_ptm_trnscr	Line card interface plug-in management
fe_ptm_virpt	Virtual port management
fe_span	SPAN service
ftp_server	Function of the FTP server service
ftpc_cli	Function of the FTP client service
igmp	Function of IGMP multicast group management service
igmp_snp	Function of IGMP multicast detection
ipv4	IPV4 function
ipv6	IPv6 function
isis	Function of ISIS routing protocol
ldpd	Function of LDP
lldpdemo	LLDP control plane function
lsm_ko	Function of interface status management kernel
lsm_rpc_agent	Function of interface status management agent
lsmdemo	Function of interface status management guard
mlag-services	Service whole set related to MLAG
mld	Function of MLD multicast group management
mld_snp	Function of MLD multicast detection
mstp	STP control plane

Module Name	Description
nsm	Function of the network service
nsm_proxy	Network service kernel agent
ntp	Function of the NTP service
ospf	Function of the OSPF service
ospfv3	Function of the OSPFv3 service
pbr	Function of the PBR service
qosd	Function of the QoS service
rdnd-proxy	Hot standby framework proxy module
reup	REUP protocol control plane
rg_syslogd	Function of the syslog service
rg-lacp	Function of the LACP service
rg-mlag	Control plane service of MLAG
rg-rdnd	Hot standby management framework
rg-snmpd	Function of the SNMP service
rg-span	Control plane function of the mirroring function
rg-sshc	Function of the SSH Client service
rg-sshd	Function of the SSH Server service
rg-sysmon	Function of the equipment monitoring service
rg-sysmon-pre	Function of the equipment monitoring service
rg-telnetc	Function of the Telnet Client service
rg-telnetd	Function of the Telnet Server service
rip	Function of the RIP service
ripng	Function of the RIPng service
rpi	Function of the routing policy service
S80psh_server	Function of the equipment self-healing service
sccd	Function of the security control center service
snooping	Functions of the DHCP detection service (DHCP snooping, IP source guard, port security, ARP-CHECK, DAI, gateway ARP anti-spooling, and global IP address + MAC address binding)

Module Name	Description
ss_proxy	Proxy process of SS
ssa_sdk	Switching chip driver
ssa_sdk_78ccm	Supervisor module switching chip driver
tcpip	TCP/IP function
tftpd	Function of the TFTP service
tftp-server	Function of the TFTP server service
tipc	Communication protocol
tipc-tap	Module for interworking with the TIPC protocol, device management, and TIPC driver
urpf	A unicast reverse routing lookup technology used to prevent network attacks based on source address spoofing
v6snooping	Function of the DHCPv6 spoofing service (DHCPv6 Snooping and IPv6 Source Guard)
vrrp	Function of the VRRP service
vrrp_plus	Function of the VRRP+ service
xe.cpp.dp	CPP all deployment module on the unified data plane

Common Errors

N/A

Platform Description

All products support this command.

Related Commands

N/A

1.2 cmdk start

Function

Run the **cmdk start** command to start a specified process of the board in a specified slot on a specified device.

Syntax

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **start**

Parameter Description

device-id: Device ID. The default value is **1**.

slot-id: Slot ID of a board.

module-name: Module name.

Table 1-3 Definitions of Slot IDs in the Command String

Slot	Slot ID
Supervisor Module 1	M1
Supervisor Module 2	M2
Interface board	Slot ID corresponding to the interface board. The value range is from 1 to 8.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is run on only the master device.
- You can run the **show version slot** command to query the device ID and user slot ID.

Examples

The following example starts the span process of the board in slot 0 on device 1.

```
Hostname> enable
Hostname# cmdk device 1 slot 0 module span start
Hostname# This operation will reset the span. Are you sure to continue? [N/y]y
```

Notifications

N/A

Common Errors

N/A

Platform Description

All products support this command.

Related Commands

N/A

1.3 cmdk stop

Function

Run the **cmdk stop** command to stop a specified process of the board in a specified slot on a specified device.

Syntax

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **stop**

Parameter Description

device-id: Device ID. The default value is **1**.

slot-id: Slot ID of a board.

module-name: Module name.

Table 1-4 Definitions of Slot IDs in the Command String

Slot	Slot ID
Supervisor Module 1	M1
Supervisor Module 2	M2
Interface board	Slot ID corresponding to the interface board. The value range is from 1 to 8.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is run on only the master device.
- You can run the **show version slot** command to query the device ID and user slot ID.

Examples

The following example stops the span process of the board card in slot 0 on device 1.

```
Hostname> enable
Hostname# cmdk device 1 slot 0 module span stop
Hostname# This operation will reset the span. Are you sure to continue? [N/y]y
```

Notifications

N/A

Common Errors

N/A

Platform Description

All products support this command.

Related Commands

N/A

1.4 cmdk detail

Function

Run the **cmdk detail** command to display the process of the board in a specified slot on a specified device.

Syntax

cmdk device *device-id* **slot** *slot-id* **detail**

Parameter Description

device-id: Device ID. The default value is **1**.

slot-id: Slot ID of a board.

Table 1-5 Definitions of Slot IDs in the Command String

Slot	Slot ID
Supervisor Module 1	M1
Supervisor Module 2	M2
Interface board	Slot ID corresponding to the interface board. The value range is from 1 to 8.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

- This command is run on only the master device.
- You can run the **show version slot** command to query the device ID and user slot ID.

Examples

The following example displays all processes of the board in slot 0 on device 1.

```
Hostname> enable
Hostname# cmdk device 1 slot 0 detail
S80psh_server
aaad
acld
aclk
adduser
adjust-memory
af_key_cli
af_key_k
ap_ko
app_identify
```

```
app_identify_ko
arp_sprs
bfd
bgp
bridge
check_config
checkfs
cli-proxy
cli-server
cmdk
cmpnt_upgrade_begin
cmpnt_upgrade_client
cmpnt_upgrade_server
congestctrl_server
--More--
```

Notifications

N/A

Common Errors

N/A

Platform Description

All products support this command.

Related Commands

N/A

1.5 debug cmdk

Function

Run the **debug cmdk** command to enable or disable the CMDK debugging mode.

The CMDK debugging mode is disabled by default.

Syntax

debug cmdk on

debug cmdk off

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example enables the CMDK debugging mode.

```
Hostname> enable
Hostname# debug cmdk on
```

Notifications

N/A

Common Errors

N/A

Platform Description

All products support this command.

Related Commands

N/A

1 Python Commands

Command	Function
Python	Debug a Python script.

1.1 Python

Function

Run the **python** command to debug a Python script.

No Python-related operation (for example, debugging a Python script or running the **Python** command) is performed by default.

Syntax

python [*file-name* | *args*]

Parameter Description

file-name: Name of a script file. The default directory for search is **flash:**. **flash:** can be added to the directory.

args: Script file parameter.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

The **copy** command is run to upload a Python script to a device.

When no parameter is included in this command, the Python console is accessed.

Examples

The following example runs a Python script named **hello.py**.

```
Hostname> enable
Hostname# python hello.py
Could not find platform dependent libraries <exec_prefix>
Consider setting $PYTHONHOME to <prefix>[:<exec_prefix>]
hello,word!
Device#
```

Notifications

N/A

Common Errors

N/A

Platform Description

Because Python occupies too much space in the flash memory, the help and license interfaces used to display the version and license information in Python are removed. But this does not affect other functions of help and license.

Related Commands

N/A

1 License Management Commands

Command	Function
license copy	Back up license files.
license grace-period	Configure the grace period before a license expires.
license install	Install a license.
license auto-install	Automatically match and install a license.
license uninstall	Uninstall a license.
license auto-uninstall	Uninstall a license.
license unbind	Unbind a license.
license update	Update a license.
show license all-license	Display the list of all installed license files in the device.
show license dev-license	Display the list of license files on each device in the system.
show license file	Display the information about a specified license file on the device.
show license hostid	Display the host ID used for licensing.
show license dev-hostid	Display the host ID used for licensing.
show license usage	Display the usage of the current license in the system.
show license unbind-code	Display the verification code of a license unbound from the local device.
show license dev-unbind-code	Display the verification code of a license unbound from each device in the system.

1.1 license copy

Function

Run the **license copy** command to back up license files.

No license file is backed up by default.

Syntax

license { **copy-all** | **copy-file** *filename* } { **flash:** | **usb0:** } [*target-filename*]

Parameter Description

copy-all: Backs up all permanent license files in the system.

copy-file: Backs up the license file specified by *filename* in the system. *filename* is the name of a license file or a feature that has been installed in the system. When *filename* is a feature name, all the installed license files for this feature are backed up.

flash: Specifies the location of a license file in the internal flash file system.

usb0: Specifies the location of a license file in the USB file system.

target-filename: Name of a license file.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- **copy-file** is used to back up either a single license file or all license files for a feature.
- When all license files in the system are backed up, a .tar file is generated.
- You can run the **dir** command to view the generated license file package. After decompressing the package, compare the license files with the license file names displayed in the **installed license** fields of permanently licensed features in the command output of the **show license all-license** command to check whether licenses are correctly backed up.
  - The **installed license** field is available only for multi-instance licenses. The name of a file internally backed up in the multi-instance license system is determined by the ID of the multi-instance license.
  - One single-instance license file exists at most in the system at a time. Therefore, the internally backed up single-instance license file is named after the feature.

Examples

The following example backs up all license files in the system to the **rg-license-lics** path (mandatory) of the USB flash drive. The license file package is named **lics.tar**.

```
Hostname> enable
Hostname# license copy-all usb0:rg-license-lics/lics.tar
Success to copy all permanent license.
```

Notifications

When you want to back up all license files but there is no license file for backup in the system, the following notification will be displayed:

```
Copy failed, there's no permanent license in the system.
```

When all license files in the system are backed up, the following notification will be displayed:

```
Success to copy all permanent license.
```

When the specified feature or license file is not on the device, the following notification will be displayed:

```
Copy failed, there’s no such service or license installed in the system.
```

When the specified license file is temporary, the following notification will be displayed:

```
Copy failed, the license is temporary.
```

When the specified license file is backed up, the following notification will be displayed:

```
Success to copy license vsd.lic.
```

Common Errors

- The specified license or file does not exist in the system.
- The backup fails as the specified license to be backed up is temporary.

Platform Description

N/A

Related Commands

N/A

1.2 license grace-period

Function

Run the **license grace-period** command to configure the grace period before a license expires.

The grace period before a license expires is 180 days by default.

Syntax

license grace-period *filename days*

Parameter Description

filename: Name of a license feature.

days: Grace period (in days) before a license expires. The range is from 0 to 365.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- A grace period is set for an evaluation license only but not a permanent license.
- When a license is going to expire in 100 days, a warning message is generated at regular intervals.
  - When the expiration time of a license is less than the grace period, a warning is generated once a day.
  - The day before a license expires, a warning is generated every hour. A warning is sent in the form of a log or SNMP trap message.

Examples

The following example configures the temporary license for the installed VSD feature in the system and sets the grace period to 100 days.

```
Hostname> enable
Hostname# license grace-period LIC-VSD 100
Success to set alarm starting point of license LIC-VSD.
```

Notifications

When the grace period is successfully set, the following notification will be displayed:

```
Success to set alarm starting point of license LIC-VSD.
```

When the specified license does not exist in the system, the following notification will be displayed:

```
There's no license abc in the system.
```

Common Errors

The specified license does not exist in the system.

Platform Description

N/A

Related Commands

N/A

1.3 license install

Function

Run the **license install** command to install a license.

Syntax

license install { **flash:** | **usb0:** } *filename*

Parameter Description

flash: Specifies the location of a license file in the internal flash file system.

usb0: Specifies the location of a license file in the USB file system.

filename: Name of a license file.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- The name of a license file can be modified.
- In a VSU environment, run the **license install** command on the master device to install a license on all devices, or run this command on a non-master device to install a license locally.

Examples

The following example installs a license file for the VSD feature.

```
Hostname> enable
Hostname# license install usb0:vsd.lic
License file install success, service name: LIC-VSD.
```

Notifications

When the license file does not exist, the following notification will be displayed:

```
Install failed: no such file or directory.
```

When the license file is invalid, the following notification will be displayed:

```
Install failed: the install license may be wrong.
```

When a license file later than the one to be installed already exists in the system, the following notification will be displayed:

```
Install failed: the system already has a same license which is newer.
```

When a license file is repeatedly installed, the following notification will be displayed:

```
Install failed: the license has been installed before.
```

When a license is temporary and a permanent license for the same feature already exists in the system, the following notification will be displayed:

```
Install failed: The system already has a same permanent license.
```

When a license (the license for the VSD feature above) is installed, the following notification will be displayed:

```
License file install success, service name: LIC-VSD.
```

When a license (the license for the VSD feature above) is installed and converted into a permanent one, the following notification will be displayed:

```
License file install success, service name: LIC-VSD.
The license turns to be permanent.
```

When a license (the license for the VSD feature above) is installed and is to be expired in less than 30 days, the following notification will be displayed:

```
License file install success, service name: LIC-VSD.;
The installed license is approaching deadline, less than 30 days.
```

Common Errors

- The specified license file does not exist.
- The license file is invalid.

- The SN of the license file does not match that of the device.
- The pre-installed license is earlier than that in the system.
- A license file is repeatedly installed.
- The pre-installed license is temporary but the system has installed a permanent license.

Platform Description

N/A

Related Commands

N/A

1.4 license auto-install

Function

Run the **license auto-install** command to automatically match and install a license.

Syntax

license auto-install { **flash:** | **usb0:** } *filename*

Parameter Description

flash:: Specifies the location of a license file in the internal flash file system.

usb0:: Specifies the location of a license file in the USB file system.

filename: Name of a license file.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- The name of a license file can be modified.
- This command is used in a VSU environment.
  - In a VSU environment, this command is used to install a license on a matched board only.
  - In a non-VSU environment, this command has the same function as the **license install** command.

Examples

The following example installs a license for the FC feature.

```
Hostname> enable
Hostname# license install usb0:fc.lic
License file install success, dev 2 install it, service name: LIC-FC-BLADE-S.
```

Notifications

When the license file does not exist, the following notification will be displayed:

```
Install failed: no such file or directory.
```

When the license file is invalid, the following notification will be displayed:

```
Install failed: the install license may be wrong.
```

When a license file later than the one to be installed already exists on the device, the following notification will be displayed:

```
Install failed: device 2 already has a same license which is newer.
```

When a license file is repeatedly installed, the following notification will be displayed:

```
Install failed: the license has been installed to device 2 before.
```

When a license is temporary and a permanent license for the same feature already exists on the device, the following notification will be displayed:

```
Install failed: device 2 already has a same permanent license.
```

When a license (the license for the FC feature above) is installed for a specific device, the following notification will be displayed:

```
License file install success, device 2 installed it, service name: LIC-FC-BLADE-S.
```

When a license (the license for the FC feature above) is installed for a specific device and converted into a permanent one, the following notification will be displayed:

```
License file install success, device 2 installed it, service name: LIC-FC-BLADE-S .
The license turns to be permanent.
```

When a license is installed (the license for the FC feature above) for a specific device and is to be expired in less than 30 days, the following notification will be displayed:

```
License file install success, device 2 installed it, service name: LIC-FC-BLADE-S .;
The installed license is approaching deadline, less than 30 days.
```

Common Errors

- The specified license file does not exist.
- The license file is invalid.
- No device matches the license file in the environment.
- The pre-installed license is earlier than that in the system.
- A license file is repeatedly installed.
- The pre-installed license is temporary but the system has installed a permanent license.

Platform Description

N/A

Related Commands

N/A

1.5 license uninstall

Function

Run the **license uninstall** command to uninstall a license.

Syntax

license uninstall *license* [*filename*]

Parameter Description

all: Uninstalls all license files in the system.

license: Name of the license to be uninstalled.

filename: Name of the file to be uninstalled.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- If the licensed feature is running, the uninstallation does not take effect immediately.
- An uninstalled license is not restored. It is recommended that you back up the license file before uninstalling it.

Examples

The following example uninstalls the VSD license in the system.

```
Hostname> enable
Hostname# license uninstall LIC-VSD
Uninstall LIC-VSD success.
```

Notifications

When the specified license file (named **defd**) does not exist on the device, the following notification will be displayed:

```
Uninstall failed: there's no license defd in the system.
```

When the specified license file (named **123.lic**) for the specified feature (LIC-WLAN-AP-32) does not exist on the device, the following notification will be displayed:

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the system.
```

When a single license file of a single-instance licensed feature is uninstalled, the following notification will be displayed:

```
Uninstall failed: single instance license does not support license based uninstalling.
```

When a license is uninstalled (for the VSD feature), the following notification will be displayed:

```
Uninstall LIC-VSD success.
```

When a single license file (named **AP32_1.lic**) of a licensed feature is (LIC-WLAN-AP-32) uninstalled, the following notification will be displayed:

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

Common Errors

- No license is installed for the specified feature on the device.

- The specified license file for the specified feature does not exist on the device.
- A license file for a single-instance feature is pre-uninstalled (a single license file is not uninstalled in a single-instance license scenario).

Platform Description

N/A

Related Commands

N/A

1.6 license auto-uninstall

Function

Run the **license auto-uninstall** command to uninstall a license.

Syntax

license auto-uninstall *device-id license* [*filename*]

Parameter Description

device-id: ID of the device that stores the file to be uninstalled.

license: Name of the license to be uninstalled.

filename: Name of the file to be uninstalled.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- If the licensed feature is running, the uninstallation will not take effect immediately.
- An uninstalled license is not restored. It is recommended that you back up the license file before uninstalling it.

Examples

The following example uninstalls the FC license in the system.

```
Hostname> enable
Hostname# license auto-uninstall 2 LIC-FC-BLADE-S
License file uninstall LIC-FC-BLADE-S of device 2 success.
```

Notifications

When the specified license (named **defd**) does not exist on the specified device (device 2, the same as below), the following notification will be displayed:

```
Uninstall failed: there's no license defd in the device 2.
```

When the specified license file (named **123.lic**) for the specified feature (LIC-WLAN-AP-32) does not exist on the specified device, the following notification will be displayed:

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in device 2.
```

When a single license file of a single-instance licensed feature is uninstalled, the following notification will be displayed:

```
Uninstall failed: single instance license does not support license based uninstalling.
```

When a license is uninstalled (for the FC feature), the following notification will be displayed:

```
Uninstall LIC-FC-BLADE-S in device 2 success.
```

When a single license file (named **AP32_1.lic**) of a licensed feature is (LIC-WLAN-AP-32) uninstalled, the following notification will be displayed:

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 in device 2 success.
```

Common Errors

- No license is installed for the specified feature on the specified device.
- The specified license file for the specified feature does not exist on the specified device.
- A license file for a single-instance feature is pre-uninstalled (a single license file is not uninstalled in a single-instance license scenario).
- The specified device does not exist.

Platform Description

N/A

Related Commands

N/A

1.7 license unbind

Function

Run the **license unbind** command to unbind a license.

Syntax

license unbind *pak*

Parameter Description

pak: License code

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

- This command is used to unbind a license file from a device. You must run this command to unbind the

license from the device before removing the binding on the website.

- Upon unbinding, you obtain a verification code, which is needed for the unbinding on the website.

Examples

The following example unbinds the license with the license code of LIC-FCOE00000012268888.

```
Hostname> enable
Hostname# license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is
775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855.
```

Notifications

When the system has no matched license, the following notification will be displayed:

```
Unbind failed: not match license found.
```

Common Errors

The system has no matched license.

Platform Description

N/A

Related Commands

N/A

1.8 license update

Function

Run the **license update** command to update a license.

Syntax

license update { **flash:** | **usb0:** } *filename*

Parameter Description

flash:: Specifies the location of a license file in the internal flash file system.

usb0:: Specifies the location of a license file in the USB file system.

filename: Name of a license file.

Command Modes

Privileged EXEC mode

Default Level

4

Usage Guidelines

N/A

Examples

The following example updates the temporary license for VSD to a permanent one.

```
Hostname> enable
Hostname# license update usb0:vsd_perm.lic
License file update success, temporary license LIC-VSD changes into permanent.
```

Notifications

When the license file does not exist, the following notification will be displayed:

```
Update failed: No such file or directory.
```

When the license file is invalid, the following notification will be displayed:

```
Update failed: the update license may be wrong.
```

When the pre-installed license is earlier than that in the system, the following notification will be displayed:

```
Update failed: the new installed license is older than the system one
```

When a license has been installed, the following notification will be displayed:

```
Update failed: the license has been installed before.
```

When a temporary license cannot replace a permanent one, the following notification will be displayed:

```
Update failed: the period license cannot replace permanent license.
```

When no license has been installed for the feature of the pre-installed license, the following notification will be displayed:

```
Update failed: now the system does not have the license.
Try "license install" instead.
```

When an evaluation license is updated and converted into a permanent one (the license for the VSD feature), the following notification will be displayed:

```
Update success, temporary license LIC-VSD changes into permanent.
```

Common Errors

- The license file is specific to the current device.
- An earlier license is used to replace a later one.
- The updated license has been installed.
- A temporary license is used to replace a permanent one.
- No license has been installed for the feature during the license update.

Platform Description

N/A

Related Commands

N/A

1.9 show license all-license

Function

Run the **show license all-license** command to display the list of all installed license files in the device.

Syntax

show license all-license

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the information about all installed licenses in the system

```
Hostname> enable
Hostname# show license all-license
Searching license in the system...
1. Service name: LIC-AP-64
   Attribute: Releasable
  [Permanent licenses]   [Licensed serial number]
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988
  [Temporary license]    [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)
2. Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
```

Table 1-1 Output Fields of the show license all-license Command

Field	Description
Service name	Name of the licensed feature
Attribute	Attributes of this license
Left days	Remaining days before expiry of the license

Field	Description
Licensed serial number	License code

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show license dev-license

Function

Run the **show license dev-license** command to display the list of license files on each device in the system.

Syntax

show license dev-license

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the information about licenses installed on each device in the system

```
Hostname> enable
Hostname# show license dev-license
Searching license in the system...
Dev 1:
1. Service name: LIC-AP-64
   Attribute: Releasable
  [Permanent licenses]   [Licensed serial number]
```

```
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988
  [Temporary license]   [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)
2. Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
Dev 2:
 1. Service name: LIC-FC-BLADE-S
   Attribute: Temporary, Releasable
   Left days: 99
   Licensed serial number: LIC-FC-BLADE-S 00000001884686
2. Service name: LIC-AP
   Attribute: Permanent, Releasable
  [Installed licenses]   [Licensed serial number]
   19880921.lic           LIC-AP00000012265001
19880922.lic           LIC-AP00000012265002
```

Table 1-2 Output Fields of the show license dev-license Command

Field	Description
Service name	Name of the licensed feature
Attribute	Attributes of this license
Left days	Remaining days before expiry of the license
Installed license	Installed license files
Licensed serial number	License code

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show license file

Function

Run the **show license file** command to display the information about a specified license file on the device.

Syntax

show license file *file-license*

Parameter Description

file-license: Information about a specified license name. *filename* indicates the name of the license file.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the information about the VSD license.

```
Hostname# show license file LIC-VSD
Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
```

Table 1-3 Output Fields of the show license file Command

Field	Description
Service name	Name of the licensed feature
Attribute	Attributes of this license
Left days	Remaining days before expiry of the license
Licensed serial number	License code

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show license hostid

Function

Run the **show license hostid** command to display the host ID used for licensing.

Syntax

show license hostid

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the host ID of a device.

```
Hostname> enable
Hostname# show license hostid
1234942570021
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show license dev-hostid

Function

Run the **show license dev-hostid** command to display the host ID used for licensing.

Syntax

show license dev-hostid

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the host ID of each device.

```
Hostname> enable
Hostname# show license dev-hostid
Dev 1: 8708EH5F00042
Dev 2: GH3002893D300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show license usage

Function

Run the **show license usage** command to display the usage of the current license in the system.

Syntax

show license usage

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the license information.

```
Hostname> enable
Hostname# show license usage
Searching license in the system...
1. Service name: LIC-AP-64
   Attribute: Releasable
  [Permanent licenses]   [Licensed serial number]
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988
  [Temporary license]    [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)
2. Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
```

Table 1-4 Output Fields of the show license usage Command

Field	Description
Service name	Name of the licensed feature
Attribute	Attributes of this license
Left days	Remaining days before expiry of the license

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show license unbind-code

Function

Run the **show license unbind-code** command to display the verification code of a license unbound from the local device.

Syntax

show license unbind-code

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the verification code of a license unbound from a device.

```
Hostname> enable
Hostname# show license unbind-code
LICENSE              UNBINDING-CODE
LIC-VSD00000012264933
77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5
LIC-FCOE00000012264966
77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5
LIC-TRILL00000012264988
77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF55FF5
```

Table 1-5 Output Fields of the show license unbind-code Command

Field	Description
LICENSE	License code of an unbound license
UNBINDING-CODE	Verification code of an unbound license

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show license dev-unbind-code

Function

Run the **show license dev-unbind-code** command to display the verification code of a license unbound from each device in the system.

Syntax

show license dev-unbind-code

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the verification codes of licenses unbound from each device in the system.

```
Hostname> enable
Hostname# show license dev-unbind-code
Searching unbound license in the system...
Dev 1:
LICENSE              UNBINDING-CODE
LIC-FCOE00000012265013
57771FF68737BFF69FF55FF557F55FF57575B5A5556587857FF59FF59765AFF55FF5
LIC-VSD00000012265011
57771FF68737BFF69FF55FF557F55FF57575B5A5556567857FF59FF59765AFF55FF5     Dev 2:
LICENSE              UNBINDING-CODE
LIC-VSD00000012264933
```

```
77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5
LIC-TRILL00000012264966
77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5
LIC-FCOE00000012264988
77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF55FF5
```

Table 1-6 Output Fields of the show license dev-unbind-code Command

Field	Description
LICENSE	License code of an unbound license
UNBINDING-CODE	Verification code of an unbound license

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 USB Command

Command	Function
show usb	Display the information about the inserted USB flash disk.
usb remove	Remove the USB flash disk.

1.1 show usb

Function

Run the **show usb** command to display the information about the inserted USB flash disk.

Syntax

show usb

Parameter Description

N/A

Command Modes

All modes except user EXEC mode

Default Level

2

Usage Guidelines

If there is a USB flash disk inserted, its information is displayed. If not, an error notification pops up.

Examples

The following example displays the information about the inserted USB flash disk.

```
Hostname> enable
Hostname# show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
```

Table 1-1 Output Fields of the show usb Command

Field	Description
Device: Mass Storage	Device name. **Mass Storage** is the USB flash disk name.
ID	Device ID.
URL prefix	URL prefix of the USB flash disk.
Disk Partitions	USB flash disk partition. **vfat** refers to FAT16 and FAT32 file system.
Size	Total size of the USB flash disk.
Available size	Available size of the USB flash disk.

Notifications

If there is no USB flash disk inserted, the following notification will be displayed:

```
No partition found.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 usb remove

Function

Run the **usb remove** command to remove the USB flash disk.

Syntax

usb remove *device-id*

Parameter Description

device_id: Device ID of the specified USB flash disk. You can run the **show usb** command to display the device ID.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

Before pulling out the USB flash disk, please run the **usb remove** command to remove the USB flash disk from the system. Otherwise, USB storage data may be corrupt.

If the USB flash disk is removed successfully, the system will show a prompt and you can pull out the device. If the USB flash disk fails to be removed, please wait a moment and try again.

Examples

The following example removes USB flash disk **0**.

```
Hostname> enable
Hostname# usb remove 0
OK, now you can pull out the device 0.
```

Notifications

If the USB flash disk is removed successfully, the following notification will be displayed:

```
OK, now you can pull out the device 0.
```

If the USB flash disk fails to be removed, the following notification will be displayed:

```
Device is busy now, try again few minutes later.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Virtualization Commands

1 VSU Commands

Command	Function
dad relay enable	Enable the forwarding of dual-active detection (DAD) packets based on aggregation port (AP).
dual-active bfd interface	Configure a BFD-based DAD port.
dual-active detection	Enable the DAD.
dual-active exclude interface	Configure an excluded port in Recovery mode for dual-active devices.
dual-active interface	Configure an AP-based DAD port.
port-member interface	Configure a VSL member port.
led-blink	Configure quick blinking location.
show switch id	Display the ID of the local device.
show switch virtual	Display the information summary of a device.
show switch virtual balance	Display the traffic balancing mode.
show switch virtual config	Display the VSU configurations.
show switch virtual dual-active	Display DAD information.
show switch virtual link	Display the VSL information.
show switch virtual role	Display the information about device roles.
show switch virtual topology	Display the information about the VSU device topology.
switch	Configure the device ID.
switch cfg_mode	Specify the manner of saving the VSU configuration file.
switch convert mode	Configure the standalone or VSU mode.
switch crc errors	Configure the CRC error detection parameter.
switch description	Configure a device name.
switch domain	Modify the domain ID of a device in VSU mode.
switch priority	Configure a device priority.
switch renumber	Modify a device ID.

switch virtual aggregateport-lff enable	Enable AP-based LFF.
switch virtual domain	Configure a VSU domain ID or enter the VSU domain configuration mode.
switch virtual ecmp-lff enable	Enable ECMP-based LFF.
vsl-port	Enter the VSL port configuration mode.
recovery auto-restart enable	Enable the automatic restart function of dual-active devices after a link fault is rectified in the recovery mode.

1.1 dad relay enable

Function

Run the **dad relay enable** command to enable the forwarding of dual-active detection (DAD) packets based on aggregation port (AP).

Run the **no** form of this command to disable the forwarding of AP-based DAD packets.

The forwarding of AP-based DAD packets is disabled by default.

Syntax

dad relay enable

no dad relay enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to enable the AP-based DAD in a VSU network and runs on a forwarding device connected to the VSU members.

Configure this command on an AP only.

Examples

The following example enables the forwarding of DAD packets on aggregate port 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregateport 1
Hostname(config-if-AggregatePort 1)# dad relay enable
```

Notifications

N/A

Common Errors

The DAD packets must be forwarded on an AP.

Platform Description

N/A

Related Commands

- **dual-active detection**

- **show switch virtual dual-active**

1.2 dual-active bfd interface

Function

Run the **dual-active bfd interface** command to configure a BFD-based DAD port.

Run the **no** form of this command to delete a BFD-based DAD port.

Syntax

dual-active bfd interface *interface-type interface-number*

no dual-active bfd interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of the BFD-based detection port.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is configured only in VSU mode.

The BFD-based detection port must be a directly connected physical port and be configured as a layer-3 routed port.

The BFD-based detection link must connect different devices (the active and standby devices only).

Examples

The following example configures the port GigabitEthernet 0/1 as the BFD-based DAD port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active bfd interface GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

The detection port is not a routed port.

Platform Description

N/A

Related Commands

- **show switch virtual dual-active**

1.3 dual-active detection

Function

Run the **dual-active detection** command to enable the DAD.

Run the **no** form of this command to disable the DAD.

The DAD is disabled by default.

Syntax

dual-active detection { **aggregateport** | **bfd** }

no dual-active detection { **aggregateport** | **bfd** }

Parameter Description

aggregateport: Enables AP-based DAD.

bfd: Enables BFD-based DAD.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is configured only in VSU mode.

If the **aggregateport** parameter is specified**,** the forwarding of AP-based DAD packets must also be enabled.

Examples

The following example enables the BFD-based DAD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active detection bfd
```

The following example enables the AP-based DAD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active detection aggregateport
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual dual-active**

1.4 dual-active exclude interface

Function

Run the **dual-active exclude interface** command to configure an excluded port in Recovery mode for dual-active devices.

Run the **no** form of this command to delete an excluded port in Recovery mode for dual-active devices.

Syntax

dual-active exclude interface *interface-type interface-number*

no dual-active exclude interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of an excluded port in Recovery mode for dual-active devices.

Command Modes

config-vs-domain configuration mode

Default Level

14

Usage Guidelines

This command is configured only in VSU mode.

Excluded ports must be routed ports but not VSL ports.

You can configure multiple excluded ports.

Examples

The following example configures the port GigabitEthernet 0/1 as an excluded port in Recovery mode for dual-active devices.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active exclude interface GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

- A VSL port is configured as an excluded port.
- An excluded port is not a routed port.

Platform Description

N/A

Related Commands

- **show switch virtual dual-active**

1.5 dual-active interface

Function

Run the **dual-active interface** command to configure an AP-based DAD port.

Run the **no** form of this command to delete an AP-based DAD port.

Syntax

dual-active interface *interface-type interface-number* [**vlan** *vlan-id*]

no dual-active interface *interface-type interface-number* [**vlan** *vlan-id*]

Parameter Description

interface-type interface-number: Type and number of a port (which must be an AP).

vlan-id: VLAN ID (VID) of a used AP. The value range is from 1 to 4094.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

Only one AP-based DAD port is configured. You must create an AP before configuring it as a detection port. The latter detection port overwrites the previous one.

When the AP is a trunk port and the native VLAN is beyond the VLAN range allowed by the AP-based detection port, configure a detection VLAN for the AP-based detection port. The configured detection VLAN must fall within the VLAN range allowed by the trunk port and have been correctly created on the device.

Examples

The following example configures aggregate port 1 as a DAD port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active interface aggregateport 1
```

The following example configures aggregate port 1 as a DAD port. This AP is a trunk port. The allowed VLAN range is from 2 to 10, and the detection VLAN is 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregateport 1
```

```
Hostname(config-if-AggregatePort 1)# switchport mode trunk
Hostname(config-if-AggregatePort 1)# switchport trunk allowed vlan only 2-10
Hostname(config-if-AggregatePort 1)# exit
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# dual-active interface aggregateport 1 vlan 10
```

Notifications

N/A

Common Errors

- The detection port is not an AP.
- The AP is configured as a trunk port with an allowed VLAN range, but no VLAN is configured for the detection port.

Platform Description

N/A

Related Commands

- **show switch virtual dual-active**

1.6 port-member interface

Function

Run the **port-member interface** command to configure a VSL member port.

Run the **no** form of this command to delete a VSL member port.

Syntax

port-member interface *interface-type interface-number*

no port-member interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of the port. The port type parameter must be a 10G port or above. The port name parameter is 2-dimensional in standalone mode, for example, the value is GigabitEthernet 0/1. It is 3-dimensional in VSU mode, for example, the value is GigabitEthernet 1/0/1.

Command Modes

VSL interface configuration mode

Default Level

14

Usage Guidelines

This command is available in both VSU and standalone modes. You must save the command configurations.

The VSL port type must be a 10G port or above.

The four 10G ports split from a 40G port cannot be configured as VSL ports.

If a common port is configured as an NLB reflex port, it can serve as a VSL port only after the service is deleted.

If the VSU topology is split when a VSL port is switched to a common port, the VSL port must not be deleted. You can disconnect the physical port and then delete the VSL port.

Examples

The following example adds/deletes the VSL member port TenGigabitEthernet 0/1 in standalone mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vsl-port
Hostname(config-vsl-port)# port-member interface TenGigabitEthernet 0/1
Hostname(config-vsl-port)# no port-member interface TenGigabitEthernet 0/1
```

The following example adds/deletes the VSL member port TenGigabitEthernet 1/0/1 in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vsl-port
Hostname(config-vsl-port)# port-member interface TenGigabitEthernet 1/0/1
Hostname(config-vsl-port)# no port-member interface TenGigabitEthernet 1/0/1
```

Notifications

N/A

Common Errors

- The VSL member ports must be 10G ports or ports with higher bandwidth for some models.
- If a port is configured as an NLB reflex port, this port can be switched to a VSL member port only after the NLB reflex port configuration is deleted.

Platform Description

The VSL port type must be a 10G port or above.

Related Commands

- **show switch virtual link**

1.7 led-blink

Function

Run the **led-blink** command to configure quick blinking location.

Quick blinking location is disabled by default.

Syntax

led-blink { **enable** | **disable** } [**device** *switch-id*]

Parameter Description

enable: Enables quick blinking location.

disable: Disables quick blinking location.

switch-id: ID of the device to be configured with quick blinking location. The value range is from 1 to 2.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

In standalone mode, you can enable or disable quick blinking location only, but not specify the **device** keyword.

In VSU mode, you can specify *switch-id* to enable/disable quick blinking location for a specified device. If **device** is not specified, quick blinking location of all devices in the VSU environment is enabled/disabled.

Quick blinking location is automatically disabled 30 minutes after it is started.

The configuration takes effect immediately and is not saved. If you perform an active/standby switch or restart the device, quick blinking location is disabled.

Examples

The following example enables quick blinking location for the local device in standalone mode.

```
Hostname> enable
Hostname# led-blink enable
```

The following example enables quick blinking location for device 2 in VSU mode.

```
Hostname> enable
Hostname# led-blink enable device 2
```

The following example enables quick blinking location for all devices in VSU mode.

```
Hostname> enable
Hostname# led-blink enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show switch id

Function

Run the **show switch id** command to display the ID of the local device.

Syntax

show switch id

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the ID of the local device in standalone mode.

```
Hostname> enable
Hostname# show switch id
Switch ID is 1
```

The following example displays the ID of the local device in VSU mode.

```
Hostname> enable
Hostname# show switch id
Switch ID is 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual**
- **show switch virtual balance**
- **show switch virtual config**
- **show switch virtual dual-active**
- **show switch virtual link**
- **show switch virtual role**
- **show switch virtual topology**

1.9 show switch virtual

Function

Run the **show switch virtual** command to display the information summary of a device.

Syntax

show switch virtual

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information summary of a device in standalone mode.

```
Hostname> enable
Hostname# show switch virtual
Current system is running in "STANDALONE" mode.
```

The following example displays the information summary of a device in VSU mode.

```
Hostname> enable
Hostname# show switch virtual
Switch_id  Domain_id   Priority   Position  Status     Role          Description
1(1)       1(1)       100(100)   LOCAL    OK        ACTIVE       switch-1
2(2)       1(1)       100(100)   REMOTE    OK        CANDIDATE     switch-2
3(3)       1(1)       100(100)   REMOTE    OK        STANDBY      switch-3
```

Table 1-1 Output Fields of the show switch virtual Command

Field	Description
Switch_id	Device ID. The value in the brackets is the current configuration, which takes effect only after the device is restarted.
Domain_id	Device domain ID. The value in the brackets is the current configuration, which takes effect only after the device is restarted.
Priority	Priority. The value in the brackets is the current configuration, which takes effect only after the device is restarted.

Field	Description
Status	Device status. The available values include: ● **OK**: normal state ● **Recovery**: recovered state ● **Leave**: on-leave state ● **Isolate**: isolated state
Role	Device roles. The available values include: ● **Active**: global active devices ● **Standby**: global standby devices ● **Candidate**: global candidate devices
Description	Device alias

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual balance**
- **show switch virtual config**
- **show switch virtual dual-active**
- **show switch virtual link**
- **show switch virtual role**
- **show switch virtual topology**

1.10 show switch virtual balance

Function

Run the **show switch virtual balance** command to display the traffic balancing mode.

Syntax

show switch virtual balance

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the traffic balancing mode of a device in standalone mode.

```
Hostname> enable
Hostname# show switch virtual balance
Current system is running in "STANDALONE" mode.
```

The following example displays the traffic balancing mode of a device in VSU mode.

```
Hostname> enable
Hostname# show switch virtual balance
Aggregate port LFF: enable
ECMP LFF: enable
```

Table 1-2 Output Fields of the show switch virtual balance Command

Field	Description
Aggregate port LFF	AP-based local forward first (LFF)
ECMP LFF	ECMP-based LFF

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual**
- **show switch virtual config**
- **show switch virtual dual-active**
- **show switch virtual link**
- **show switch virtual role**

- show switch virtual topology

1.11 show switch virtual config

Function

Run the **show switch virtual config** command to display the VSU configurations.

Syntax

show switch virtual config [*switch-id*]

Parameter Description

switch-id: ID of the device whose VSU configurations are to be displayed. The value range is from 1 to 2.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the VSU configurations in standalone mode.

```
Hostname> enable
Hostname# show switch virtual config
mac: 00d0.f810.3323
!
switch virtual domain 1
!
switch 1
switch 1 priority 100
!
!
switch convert mode standalone
!
```

The following example displays the VSU configurations in VSU mode.

```
Hostname> enable
Hostname# show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
```

```
switch 1 description switch1
!
vsl-port
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
Switch convert mode virtual
!
switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
switch 2 description switch2
!
vsl-port
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
Switch convert mode virtual
!
```

The following example displays the VSU configurations of device 1.

```
Hostname> enable
Hostname# show switch virtual config 1
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-port
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
```

Table 1-3 Output Fields of the show switch virtual config Command

Field	Description
switch_id	Device ID
switch virtual domain	Domain ID of a device
priority	Device priority

Field	Description
description	Device descriptor
vsl-port	VSL port configuration

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show switch id
- show switch virtual
- show switch virtual balance
- show switch virtual dual-active
- show switch virtual link
- show switch virtual role
- show switch virtual topology

1.12 show switch virtual dual-active

Function

Run the **show switch virtual dual-active** command to display DAD information.

Syntax

show switch virtual dual-active { **aggregateport** | **bfd** | **summary** }

Parameter Description

aggregateport: Indicates the AP-based DAD configuration information.

bfd: Indicates the BFD-based DAD configuration information.

summary: Indicates the information summary of the DAD.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information summary of the DAD.

```
Hostname> enable
Hostname# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: No
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
GigabitEthernet 1/0/4
In dual-active recovery mode: No
```

The following example displays the BFD-based DAD configuration information.

```
Hostname> enable
Hostname# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
GigabitEthernet 1/0/1: UP
GigabitEthernet 2/0/2: UP
```

The following example displays the AP-based DAD configuration information.

```
Hostname> enable
Hostname# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
AggregatePort 1: UP
: GigabitEthernet 1/0/1: UP
: GigabitEthernet 2/0/1: UP
: GigabitEthernet 1/0/2: UP
: GigabitEthernet 2/0/2: UP
DAD relay enable AP list:
AggregatePort 1
```

Table 1-4 Output Fields of the show switch virtual dual-active Command

Field	Description
BFD dual-active detection enabled	Indicates whether the BFD-based DAD is enabled.
Aggregateport dual-active detection enabled	Indicates whether the AP-based DAD is enabled.
Interfaces excluded from shutdown in recovery mode	Indicates excluded ports in Recovery mode for dual-active devices.
BFD dual-active interface configured	Configures the BFD-based DAD port.
Aggregateport dual-active interface configured	Configures the AP-based DAD port.

Field	Description
DAD relay enable AP list	Indicates the list of ports for forwarding DAD packets

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual**
- **show switch virtual balance**
- **show switch virtual config**
- **show switch virtual link**
- **show switch virtual role**
- **show switch virtual topology**

1.13 show switch virtual link

Function

Run the **show switch virtual link** command to display the VSL information.

Syntax

show switch virtual link [**port**]

Parameter Description

port: Checks the status of a VSL member port.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the VSL information.

```
Hostname> enable
Hostname# show switch virtual link
VSL-AP  State  Peer-VSL    Rx      Tx        Uptime
1/1     UP     2/1       100000   100000    1d,4h,29m
2/1     UP     1/1       100000   100000    1d,4h,29m
```

Table 1-5 Output Fields of the show switch virtual link Command

Field	Description
VSL-AP	VSL AP list
State	Status of a member port. The available values include: ● **DOWN**: The port is in the link down state. ● **DISABLE**: A Cyclic Redundancy Check (CRC) error occurs on the port. ● **UP**: The port is in the link up state, but no valid VSL-AP member port is detected at the peer end. ● **OK**: The port is in the link up state, and a valid VSL-AP member port is detected at the peer end.
Peer-VSL	VSL-AP member port at the peer end.
Rx	Size of a received packet, in bytes.
Tx	Size of a transmitted packet, in bytes.
Uptime	AP connection duration

The following example displays the VSL port information.

```
Hostname> enable
Hostname# show switch virtual link port
switch 1:
Port                       AP  State  Peer-port          Rx    Tx    Uptime
TenGigabitEthernet 1/0/1   1   OK     TenGigabitEthernet 2/0/1 9000  9000  0d,0h,20m
TenGigabitEthernet 1/0/2   2   OK     TenGigabitEthernet 2/0/2 9000  9000  0d,0h,20m
Switch 2:
Port                       AP  State  Peer-port           Rx    Tx    Uptime
TenGigabitEthernet 2/0/1   1   OK     TenGigabitEthernet 1/0/1 9000  9000  0d,0h,20m
TenGigabitEthernet 2/0/2   2   OK     TenGigabitEthernet 1/0/2 9000  9000  0d,0h,20m
```

Table 1-6 Output Fields of the show switch virtual link port Command

Field	Description
Port	Port list
State	Port status
Peer-port	Peer port
Rx	Size of a received packet, in bytes

Tx	Size of a transmitted packet, in bytes
Uptime	VSL port connection duration, in minutes

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual**
- **show switch virtual balance**
- **show switch virtual config**
- **show switch virtual dual-active**
- **show switch virtual role**
- **show switch virtual topology**

1.14 show switch virtual role

Function

Run the **show switch virtual role** command to display the information about device roles.

Syntax

show switch virtual role

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command has the same function as the **show switch virtual** command.

Examples

The following example displays device roles in standalone mode.

```
Hostname> enable
Hostname# show switch virtual role
Current system is running in "STANDALONE" mode.
```

The following example displays device roles in VSU mode.

```
Hostname> enable
Hostname# show switch virtual role
Switch_id  Domain_id   Priority   Position  Status    Role        Description
1(1)       1(1)       100(100)   LOCAL     OK        ACTIVE      switch-1
2(2)       1(1)       100(100)   REMOTE    OK        CANDIDATE   switch-2
3(3)       1(1)       100(100)   REMOTE    OK        STANDBY     switch-3
```

Table 1-7 Output Fields of the show switch virtual role Command

Field	Description
Switch_id	Device ID. The value in the brackets is a modified value, which takes effect only after the device is restarted.
Domain_id	Device domain ID. The value in the brackets is a modified value, which takes effect only after the device is restarted.
Priority	Priority. The value in the brackets is a modified value, which takes effect only after the device is restarted.
Status	Device status. The available values include: ● **OK**: normal state ● **Recovery**: recovered state. ● **Leave**: on-leave state.. **Isolate**: isolated state.
Role	Device roles. The available values include: ● **Active**: global active devices ● **Standby**: global standby device **Candidate**: global candidate devices
Description	Device alias

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show switch id
- show switch virtual
- show switch virtual balance
- show switch virtual config
- show switch virtual dual-active
- show switch virtual link
- show switch virtual topology

1.15 show switch virtual topology

Function

Run the **show switch virtual topology** command to display the information about the VSU device topology.

Syntax

show switch virtual topology

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information about the VSU device topology.

```
Hostname> enable
Hostname# show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport num.
Chain Topology:
[1](1/2)-(2/1)[2]
Switch[1]: master, MAC: 00d0.f822.33d6, Description: Switch1
Switch[2]: standby, MAC: 1234.5678.9003, Description: Switch2
```

Table 1-8 Output Fields of the show switch virtual topology Command

Field	Description
Chain/Ring Topology	Topology shape, including chain topology and ring topology

Field	Description
Switch[-]	Information about a member device, including the role, MAC address, and device description

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual**
- **show switch virtual balance**
- **show switch virtual config**
- **show switch virtual dual-active**
- **show switch virtual link**
- **show switch virtual role**

1.16 switch

Function

Run the **switch** command to configure the device ID.

Run the **no** form of this command to restore the device ID to its default value.

The default device ID is 1.

Syntax

switch *switch-id*

no switch

Parameter Description

switch-id: ID of a device in VSU mode. The value range is from 1 to 2.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

A device ID is used to uniquely identify a member device of a VSU. In VSU mode, the name format of an interface is changed from "slot/port" to "switch/slot/port", where "switch" indicates the ID of the device to which the interface belongs.

If two active devices exist or if two devices are just started up with no role assigned and the devices share the same priority, the device with a smaller device ID is elected as the active one.

This command is used to modify the device ID in standalone mode only. In VSU mode, you need to run the **switch** *switch-id* **renumber** *new-switch-id* command to modify the device ID. The modified ID takes effect only after the device is restarted in both standalone mode and VSU mode.

Examples

The following example sets the ID of a device in VSU device domain 1 to 2 in standalone mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch id**
- **show switch virtual config**

1.17 switch cfg_mode

Function

Run the **switch cfg_mode** command to specify the manner of saving the VSU configuration file.

Run the **no** form of this command to restore the default configuration.

By default, the VSU configuration file of a device is separately saved and named **config_vsu.dat**.

Syntax

switch cfg_mode { **normal** | **single** }

no switch cfg_mode

Parameter Description

normal: Indicates that the VSU configuration file is separately saved and named as **config_vsu.dat**.

single: Indicates that the VSU configuration file is not separately saved and is named **config.text**.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

Examples

The following example saves the VSU configuration file to the **config.text** file in standalone mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch cfg_mode single
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual**
- **show switch virtual config**

1.18 switch convert mode

Function

Run the **switch convert mode** command to configure the standalone or VSU mode.

A device works in standalone mode by default.

Syntax

switch convert mode { **virtual** | **standalone** } [*switch-id*]

Parameter Description

virtual: Indicates the VSU mode.

standalone: Indicates the standalone mode.

switch-id: Device ID. The value range is from 1 to 2.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After you run the **switch convert mode virtual** command, the device automatically backs up each VSD global configuration file in standalone mode into a file named **vsd.standalone.text.***VSD serial number.* Then, the device clears each VSD global configuration file **config.text**, prompts you to choose whether to overwrite the VSD global configuration file **config.text** with **vsd.standalone.text.***VSD serial number*, saves the VSU configurations and restarts.

After you run the **switch convert mode standalone** command, the active device backs up each VSD global configuration file in VSU mode into a file named **vsd.virtual_switch.text.***VSD serial number.* Then, the device clears each VSD global configuration file **config.text**, prompts you to choose whether to overwrite the VSD global configuration file **config.text** with **vsd.virtual_switch.text.***VSD serial number*, and finally restarts.

This command can be run in either standalone mode or VSU mode. When this command is run in standalone mode, the work mode of the local device is switched. When this command is run in VSU mode with *switch-id* specified, the work mode of the device corresponding to *switch-id* is switched; if *switch-id* is not specified, the work mode of the active device is switched. You are advised to switch the work mode of the standby device and that of the active device.

Examples

The following example switches to the VSU mode from the standalone mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch convert mode virtual
```

The following example switches standby device 2 and active device 1 to the standalone mode successively from the VSU mode.

```
Hostname> enable
Hostname# switch convert mode standalone 2
Hostname# switch convert mode standalone 1
```

Notifications

When you switch the VSU mode to the standalone mode:

The following notification will be displayed, asking you whether to back up **config.text** as **standalone.text**, delete **config.text**, and then restart the device:

```
Convert mode will backup and delete config file, and reload the switch. Are you sure
to continue[yes/no]
```

The following notification will be displayed, asking you whether to restore **config.text** from the backup file:

```
Do you want to recover config file from back file in standalong mode (press 'ctrl +
c' to cancel) [yes/no]:n
```

When you switch the standalone mode to the VSU mode:

The following notification will be displayed, asking you whether to back up **config.text** as **virtual_switch.text**, delete **config.text**, and then restart the device:

```
Convert mode will backup and delete config file, and reload the switch. Are you sure
to continue[yes/no]
```

The following notification will be displayed, asking you whether to restore **config.text** from the backup file:

```
Do you want to recover config file from back file in standalong mode (press 'ctrl +
c' to cancel) [yes/no]:
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual config**

1.19 switch crc errors

Function

Run the **switch crc errors** command to configure the CRC error detection parameter.

Run the **no** form of this command to restore the default configuration.

By default, one CRC error occurrence is recorded if the number of CRC errors incremented between two checks is 3 or more. If 10 consecutive CRC error occurrences is recorded, take actions.

Syntax

switch crc errors *error-number* **times** *time-number*

no switch crc

Parameter Description

error-number: Threshold of CRC errors incremented between two checks. One CRC error occurrence is recorded if the number of CRC errors exceeds this threshold.

time-number: Number of consecutive CRC error occurrences.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the CRC error detection rule as follows: One CRC error occurrence is recorded if the number of CRC errors incremented between two checks is 10 or more. If 5 consecutive CRC error occurrences are recorded, the port is considered abnormal.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch crc errors 10 times 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual config**

1.20 switch description

Function

Run the **switch description** command to configure a device name.

Run the **no** form of this command to delete a device name.

No device name is configured by default.

Syntax

switch *switch-id* **description** *device-name*

no switch *switch-id* **description**

Parameter Description

switch-id: ID of the device to be configured with a name. The value range is from 1 to 2.

device-name: Device name, containing up to 32 characters.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is available in both the standalone mode and VSU mode. The configuration takes effect immediately.

Examples

The following example sets the name of device 1 to **buildingA**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 description buildingA
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual role**
- **show switch virtual config**

1.21 switch domain

Function

Run the **switch domain** command to modify the domain ID of a device in VSU mode.

Run the **no** form of this command to restore the domain ID of a device in VSU mode to its default value.

The default device domain ID is 100 in VSU mode.

Syntax

switch *switch-id* **domain** *new-domain-id*

no switch *switch-id* **domain**

Parameter Description

switch-id: ID of the running device in VSU mode. The value range is from 1 to 2.

new-domain-id: New domain ID. The value range is from 1 to 255.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is available only in VSU mode and the configuration takes effect only after device restart.

Examples

The following example modifies the domain ID of device 1 to 10 in VSU mode.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 domain 10
```

The following example restores the domain ID of device 2 to its default value (**100**) in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# no switch 2 domain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual role**
- **show switch virtual config**

1.22 switch priority

Function

Run the **switch priority** command to configure a device priority.

Run the **no** form of this command to restore the device priority to its default value.

The default device priority is **100**.

Syntax

switch *switch-id* **priority** *priority*

no switch *switch-id* **priority**

Parameter Description

switch-id: ID of the device to be configured with a priority. The value range is from 1 to 2.

priority: Device priority. The value range is from 1 to 255.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

A larger value indicates a higher priority. The device with a higher priority is elected as the active device.

You can run this command in the standalone or VSU mode. The changed priority takes effect only after device restart.

This command does not change the value of *switch-id*. In VSU mode, *switch-id* indicates the ID of the running device. If the device ID does not exist, the configuration does not take effect.

Examples

The following example sets the priority of device 1 to 200 in standalone mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 priority 200
```

The following example sets the priority of device 1 to 200 and restores the priority of device 2 to the default value (**100**) in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 priority 200
Hostname(config-vs-domain)# no switch 2 priority
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual role**
- **show switch virtual config**

1.23 switch renumber

Function

Run the **switch renumber** command to modify a device ID.

Run the **no** form of this command to restore the device ID to its default value.

The default device ID is **1**.

Syntax

switch *switch-id* **renumber** *new-switch-id* [**force**]

no switch *switch-id*

Parameter Description

switch-id: ID of the running device in VSU mode. The value range is from 1 to 2.

new-switch-id: Modified device ID. The value range is from 1 to 2.

force: Specifies whether to forcibly modify the device ID.

Warning

A confirmation message is displayed when the **force** parameter is added. If you enter **yes**, the VSU configuration is saved immediately and the device is restarted to validate the new device ID.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is available only in VSU mode and the configuration takes effect only after device restart.

Examples

The following example changes the ID of the running device 1 to 2 in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 renumber 2
```

The following example restores the ID of the running device 2 to its default value (**1**) in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# no switch 2
```

The following example forcibly modifies the ID of the running device 1 to 2 in VSU mode. Upon the modification, a confirmation message is displayed. You can enter **yes** to immediately save the configuration and restart the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# switch 1 renumber 2 force
```

Notifications

When the device ID is modified, the following notification will be displayed:

```
Renumber switch id may lead to loss of configuration and restart to connect other VSU
switch, do you want to continue? [no/yes]
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual role**
- **show switch virtual config**

1.24 switch virtual aggregateport-lff enable

Function

Run the **switch virtual aggregateport-lff enable** command to enable AP-based LFF.

Run the **no** form of this command to disable AP-based LFF.

AP-based LFF is enabled by default.

Syntax

switch virtual aggregateport-lff enable

no switch virtual aggregateport-lff enable

Parameter Description

N/A

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables AP-based LFF in VSU mode, that is, adopts the cross-device traffic balancing mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# no switch virtual aggregateport-lff enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual balance**

1.25 switch virtual domain

Function

Run the **switch virtual domain** command to configure a VSU domain ID or enter the VSU domain configuration mode.

Run the **no** form of this command to delete the VSU domain ID.

The default VSU domain ID is **100**.

Syntax

switch virtual domain *domain-id*

no switch virtual domain

Parameter Description

domain-id: VSU domain ID. The value range is from 1 to 255.

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

Only devices with the same domain ID compose a VSU. The domain ID must be unique in the LAN.

Examples

The following example sets the VSU domain ID to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show switch virtual config**
- **show switch virtual role**

1.26 switch virtual ecmp-lff enable

Function

Run the **switch virtual ecmp-lff enable** command to enable ECMP-based LFF.

Run the **no** form of this command to disable ECMP-based LFF.

ECMP-based LFF is enabled by default.

Syntax

switch virtual ecmp-lff enable

no switch virtual ecmp-lff enable

Parameter Description

N/A

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following examples disables ECMP-based LFF in VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# no switch virtual ecmp-lff enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show switch virtual balance

1.27 vsl-port

Function

Run the **vsl-port** command to enter the VSL port configuration mode.

Syntax

vsl-port

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command in the standalone or VSU mode.

Examples

The following example enters the VSL port configuration mode in standalone/VSU mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vsl-port
Hostname(config-vsl-port)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show switch virtual config
- show switch virtual link

1.28 recovery auto-restart enable

Function

Run the **recovery auto-restart enable** command to enable the automatic restart function of dual-active devices after a link fault is rectified in the recovery mode.

Run the **no** form of this command to disable the automatic restart function of dual-active devices after a link fault is rectified in the recovery mode.

By default, the automatic restart function of dual-active devices is enabled after the link fault is rectified in the Recovery mode.

Syntax

recovery auto-restart enable

no recovery auto-restart enable

Parameter Description

N/A

Command Modes

VSU domain configuration mode

Default Level

14

Usage Guidelines

This command is available in VSU mode.

Examples

The following example disables the automatic restart function of dual-active devices after a link fault is rectified in the Recovery mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switch virtual domain 1
Hostname(config-vs-domain)# no recovery auto-restart enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Interface Commands

1 Ethernet Interface Commands

Command	Function
bandwidth	Configure the bandwidth of an Ethernet interface.
carrier-delay	Configure the carrier delay of an Interface.
clear counters	Clear the interface counter.
clear link-state-change statistics	Clear the statistics about the link state change times of the interface.
define interface-range	Configure batch interface macro names.
description	Configure the interface description.
duplex	Configure the duplex mode of an interface.
errdisable recovery	Recover a port from the errdisable state.
ethernet-port counter sample-period	Configure the sampling period of Ethernet interface statistics.
ethernet-subport counter route-sample-period	Configure the sampling period of Ethernet sub-interface statistics.
fec mode	Configure the forward error correction (FEC) mode of an interface.
fiber antifake enable	Enable the optical module antifake detection function.
flowcontrol	Configure interface flow control.
flow-statistics include-interframe enable	Enable the function of including interframe gaps in interface packet rate statistics.
interface	Enter the interface configuration mode.
interface range	Batch configure interfaces.
load-interval	Configure the interval of load calculation for an interface.
logging	Configure interface information printing.
mtu	Configure the maximum transmission unit (MTU) of an interface.

mtu forwarding	Configure the forwarding plane MTU.
negotiation mode	Configure the interface auto negotiation mode.
physical-port dither protect	Configure port flapping protection.
port speed-mode	Configure the working rate mode of the 25 Gbps port.
protected-ports route-deny	Configure L3 routing blocking between protected ports.
show interfaces	View the details of an interface.
show interfaces counters	View the statistics of packets received and sent by an interface.
show interfaces counters rate physical-layer	View the packet receiving and sending rate information of an interface at the physical layer.
show interfaces link-state-change statistics	View the change time and count of the interface link state.
show interfaces mtu forwarding	View information about the forwarding plane MTU.
show interfaces status	View the status information of an interface.
show interfaces status err-disabled	View the errdisable status information of an interface.
show interfaces transceiver	View the optical module information of an interface.
show interfaces usage	View the bandwidth usage of an interface.
show mgmt virtual	View the information of the virtual management port.
show split summary	View the splitting/combining information of an interface.
shutdown	Shut down a specific interface.
snmp trap link-status	Enable the LinkTrap notification sending function for interface status change.
snmp-server if-index persist	Enable the interface index persistence function.
speed	Configure the rate of an interface.
split interface	Configure the interface splitting function.
statistics	Enable the interface traffic statistics collection and IP traffic statistics collection functions.
switchport	Configure the L2 mode for an interface.
switchport protected	Configure a port as protected port.

system mtu	Configure the MTU of the system.

1.1 bandwidth

Function

Run the **bandwidth** command to configure the bandwidth of an Ethernet interface.

Run the **no** form of this command to restore the default configuration.

No interface bandwidth is configured by default.

Syntax

bandwidth *kilobits*

no bandwidth

Parameter Description

kilobits: Interface bandwidth, in kilobits. The value range is from 1 to 2147483647.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The **bandwidth** command cannot actually affect the bandwidth of an interface. It allows the user to inform the system of the bandwidth of the interface. The bandwidth of the Ethernet interface is determined according to the rate of the actual port link by default. If necessary, the user can specify the bandwidth. **Bandwidth** is only a routing parameter and does not affect the real bandwidth of the interface of the physical link.

Examples

The following example configures the bandwidth parameter of the interface GigabitEthernet 0/1 to 64 Kbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# bandwidth 64
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 carrier-delay

Function

Run the **carrier-delay** command to configure the carrier delay of an Interface.

Run the **no** form of this command to restore the default configuration.

The default carrier delay of an interface is 2s.

Syntax

carrier-delay { [**milliseconds**] *delay-interval* | **up** [**milliseconds**] *up-interval* **down** [**milliseconds**] *down-interval* }

no carrier-delay

Parameter Description

milliseconds: Millisecond-level delay, in milliseconds. The value range is from 0 to 60000, and the value must be an integral multiple of 100.

Delay-interval: Second-level carrier delay of the interface, in seconds. The value range is from 0 to 60.

up *up-interval*: Second-level delay after which the state of the data carrier detect (DCD) signal changes from **Down** to **Up**, in seconds. The value range is from 0 to 60.

down *down-interval*: Second-level delay after which the state of the DCD signal changes from **Up** to **Down**, in seconds. The value range is from 0 to 60.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The carrier delay refers to the delay after which the DCD signal changes from **Down** to **Up** or from **Up** to **Down**. If the DCD status changes during the delay, the system will ignore this change to avoid re-negotiation on the upper data link layer.

If the DCD carrier is interrupted for a long time, the carrier delay should be set longer to accelerate route summarization and convergence of the routing table. On the contrary, if the DCD carrier interruption time is shorter than the route summarization time, the carrier delay should be set to a greater value to avoid route flapping.

Examples

The following example sets the carrier delay of the interface to 5s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# carrier-delay 5
```

The following example sets the carrier delay of the interface to 100 milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# carrier-delay milliseconds 100
```

The following example sets the delay after which the state of the DCD changes from **Down** to **Up** to 100 milliseconds and that after which the state of the DCD changes from **Up** to **Down** to 200 milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# carrier-delay up milliseconds 100 down
milliseconds 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 clear counters

Function

Run the **clear counters** command to clear the interface counter.

Syntax

clear counters [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Type and number of the interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can run the **show interfaces** command to view the statistics of the interface and run the **clear counters** command to clear the statistics of the interface in the privileged EXEC mode. If no interface is specified, all the interface counters will be cleared.

If you run the command to clear all the interface counters, it is possible that the statistics of the aggregate port (AP) are not cleared. In this case, run the **clear counters** command again, and a shorter statistics sampling period will increase the probability of such a problem.

Examples

The following example clears the counter of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear counters GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.4 clear link-state-change statistics

Function

Run the **clear link-state-change statistics** command to clear the statistics about the link state change times of the interface.

Syntax

clear link-state-change statistics *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of the interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can view the link state change statistics of the interface using the **show interfaces link-state-change** command and clear the statistics about the link state change times of the interface using the **clear link-state-change statistics** command in the privileged EXEC mode. If no interface is specified, all the interface counters will be cleared.

Examples

The following example clears the link state change statistics of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear link-state-change statistics GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 define interface-range

Function

Run the **define interface-range** command to configure batch interface macro names.

Run the **no define interface-range** command to delete batch interface macro names.

No batch interface macro names are configured by default.

Syntax

define interface-range *macro-name interface-type interface-range-string*

no define interface-range *macro-name*

Parameter Description

interface-type:-type: Interface type.

interface-range-string: Range of interface number, for example, **0/1-5** or **0/1, 0/3-4**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the macro name of the physical ports GigabitEthernet 0/1, GigabitEthernet 0/3, and GigabitEthernet 0/4 to **office201-port**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# define interface-range office201-port GigabitEthernet 0/1,0/3-4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 description

Function

Run the **description** command to configure the interface description.

Run the **no** form of this command to delete the configured interface description.

Syntax

description *interface-description*

no description

Parameter Description

interface-description: Interface description.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The **show interfaces** command is used to display the interface description and other information.

Examples

The following example configures the description of the interface GigabitEthernet 0/1 as **GBIC-1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# description GBIC-1
```

Notifications

If the length of the interface description exceeds 80 characters, an error is displayed.

```
% The length of description is up to 80!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 duplex

Function

Run the **duplex** command to configure the duplex mode of an interface.

Run the **no** form of this command to restore the default configuration.

The interface is in auto-negotiation mode.

Syntax

duplex { **auto** | **full** | **half** }

no duplex

Parameter Description

Auto: Auto negotiation.

full: Full duplex.

Half: Half duplex.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The duplex mode of an interface is related to the interface type. You can run the **show interfaces** command to view the duplex configuration of the interface.

Examples

The following example configures the full duplex mode for the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# duplex full
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 errdisable recovery

Function

Run the **errdisable recovery** command to recover a port from the errdisable state.

The port errdisable recovery function is disabled by default.

Syntax

errdisable recovery [**interval** *interval* | **cause** *link-state*]

Parameter Description

interval *interval*: Interval of automatic recovery, in seconds. If the parameter is not configured, it indicates manual recovery. Automatic recovery is unavailable. The value range is from 30 to 86400.

cause *link-state*: Recovers the interface that is set to the errdisable state by the Rapid Ethernet Uplink Protection Protocol (REUP) link tracking group function.

Command Modes

Global configuration mode

Privileged EXEC mode

Interface configuration mode

Default Level

14

Usage Guidelines

When a violation occurs, you can run the **show interfaces status err-disable** command to view the cause. After the network fault is eliminated, you can run this command to recover the interface.

The interval of automatic recovery cannot be configured in privileged EXEC mode.

Specific errdisable recovery cannot be configured in interface configuration mode.

Examples

The following example configures global port errdisable recovery.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# errdisable recovery
```

The following example recovers the port that is set to the errdisable state by the REUP link tracking group function.

```
Hostname> enable
Hostname # errdisable recovery cause link-state
```

The following example recovers the port GigabitEthernet 0/1 from the errdisable state and sets the interval of automatic recovery to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# errdisable recovery interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ethernet-port counter sample-period

Function

Run the **ethernet-port counter sample-period** command to configure the sampling period of Ethernet interface statistics.

The default sampling period of Ethernet interface statistics is 5s.

Syntax

ethernet-port counter sample-period [*interval*]

Parameter Description

Interval: Sampling interval of Ethernet interface statistics, in seconds. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Note that a shorter sampling period indicates higher system resource consumption. After completing the configuration, check the CPU usage.

Examples

The following example configures the sampling period of Ethernet interface statistics to 1s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ethernet-port counter sample-period 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ethernet-subport counter route-sample-period

Function

Run the **ethernet**-**subport counter route**-**sample**-**period** command to configure the sampling period of Ethernet sub-interface statistics.

Run the **no** form of this command to restore the default configuration.

The default sampling period of Ethernet sub-interface statistics is 5s.

Syntax

ethernet-**subport counter route**-**sample**-**period** [*interval*]

no ethernet-**subport counter route**-**sample**-**period**

Parameter Description

Interval: Sampling interval of Ethernet sub-interface statistics, in seconds. The value range is from 1 to 60.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Note that a shorter sampling period indicates higher system resource consumption. After completing the configuration, check the CPU usage.

Examples

The following example configures the sampling period of Ethernet sub-interface statistics to 1s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ethernet-subport counter route-sample-period 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 fec mode

Function

Run the **fec mode** command to configure the forward error correction (FEC) mode of an interface.

Run the **no** form of this command to restore the default configuration.

By default, the FEC mode of an interface depends on the interface type, and a specific FEC mode is subject to the actual product.

Syntax

fec mode { **rs** | **base-r** | **none** | **auto** }

no fec mode

Parameter Description

rs: Enables the FEC function as Reed-Solomon (RS)-FEC.

base-r: Enables the FEC function as BASE-R FEC.

none: Disables the FEC function.

auto: Indicates that the FEC mode is adaptive, that is, whether the FEC function is enabled or disabled is determined by the inserted optical module and its rate.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the FEC function is enabled at one end of the link, it must be also enabled at the other end.

On the premise of not affecting the negotiation status of the two ends, you are advised to:

- disable the FEC function on the QSFP28-100G-LR4 optical module, on which the FEC function is disabled by default;
- enable the FEC function on QSFP28 modules (except QSFP28-100G-LR4), on which the FEC function is enabled by default.

Examples

The following example enables the FEC function as RS-FEC for the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# fec mode rs
```

The following example enables the FEC function as BASE-R FEC for the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# fec mode base-r
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 fiber antifake enable

Function

Run the **fiber antifake enable** command to enable the optical module antifake detection function.

Run the **no** form of this command to disable the optical module antifake detection function.

The optical module antifake detection function is disabled by default.

Syntax

fiber antifake { **ignore** | **enable** }

no fiber antifake enable

Parameter Description

ignore: Disables the optical module antifake detection function.

enable: Enables the optical module antifake detection function.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An optical module alarm is printed when the optical module antifake detection function is enabled, and the system detects insertion of an optical module not supplied by Ruijie Networks. The optical module antifake detection function can be configured only for specific batches of optical modules. A false alarm may be reported for Ruijie optical modules of earlier versions.

Examples

The following example enables the optical module antifake detection function for the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# fiber antifake enable
```

Notifications

The following notification is displayed when an optical module not supplied by Ruijie Networks is inserted into the interface GigabitEthernet 0/50:

```
*Aug 6 10:11:51: %OPTICAL_MODULE-WARNING: The Optical Module(Serial Number:
G1GD3B900102B) inserted into interface GigabitEthernet 0/50 is not original Optical
Module.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 flowcontrol

Function

Run the **flowcontrol** command to configure interface flow control.

Run the **no** form of this command to restore the default configuration.

Flow control is disabled by default.

Syntax

flowcontrol { **auto** | **off** | **on** | **receive** { **auto** | **off** | **on** } | **send** { **auto** | **off** | **on** } }

no flowcontrol

Parameter Description

auto: Automatic flow control.

off: Disables flow control.

on: Enables flow control.

receive: Receiving direction of asymmetric flow control.

send: Sending direction of asymmetric flow control.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the **show interfaces** command to check whether the configuration takes effect.

Examples

The following example enables the flow control function on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# flowcontrol on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 flow-statistics include-interframe enable

Function

Run the **flow-statistics include-interframe enable** command to enable the function of including interframe gaps in interface packet rate statistics.

Run the **no** form of this command to disable the function of including interframe gaps in interface packet rate statistics.

The function of including interframe gaps in interface packet rate statistics is disabled by default.

Syntax

flow-statistics include-interframe enable

no flow-statistics include-interframe enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

All the interface rate statistics are cleared and recalculated after you run the command.

Examples

The following example enables the function of including interframe gaps in interface packet rate statistics.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# flow-statistics include-interframe enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 interface

Function

Run the **Interface** command to enter the interface configuration mode.

Syntax

interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of the interface.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enter the interface configuration mode. Then you can modify the interface configuration.

For a virtual interface, you do not need to enter the slot number when entering the interface number. Instead, you can directly enter the number of the virtual interface, for example, interface looback 0.

The support to parameters varies for the L2 and L3 interfaces. The actual support conditions of products prevail.

Examples

The following example enters the configuration mode of the physical port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#
```

The following example enters the configuration mode of the logical interface VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 interface range

Function

Run the **Interface range** command to batch configure interfaces.

The function is not configured by default.

Syntax

Interface range { *interface-type interface-range-string* } | **macro** *macro-name* }

Parameter Description

interface-type: Type of the interface. The interface can be an Ethernet physical port or a loopback interface.

interface-range-string: Range of interface number, for example, **0/1-5** or **0/1, 0/3-4**.

macro *macro-name*: Defines a macro to indicate the interface range. Here, **macro-name** is the name of the macro.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Before using a macro, you need to run the **define interface-range** command to define the interface range as *macro-name* in global configuration mode, and then run the **interface range macro** *macro-name* command to apply the macro.

Examples

The following example batch sets the interface description of GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/4 to **Office-201**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface range GigabitEthernet 0/1-2,0/4
Hostname(config-if-range)# description Office-201
```

The following example defines the interface macro name of GigabitEthernet 0/1 and GigabitEthernet 0/2 as **BW100**, and batch sets the bandwidth parameter to 100 Kbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# define interface-range BW100 GigabitEthernet 0/1-2
Hostname(config)# interface range macro BW100
Hostname(config-if-range)# bandwidth 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 load-interval

Function

Run the **load-interval** command to configure the interval of load calculation for an interface.

Run the **no** form of this command to restore the default configuration.

The default interval of load calculation for an interface is 10s.

Syntax

load-interval *interval*

no load-interval

Parameter Description

interval: Interval of load calculation for the interface, in seconds. The value range is from 5 to 600.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run this command to specify the time interval for calculating the load of packet input and output for an interface. Generally, the numbers of input/output packets and bits per second are calculated every 10 seconds. For example, if this parameter is changed to 180 seconds on the interface GigabitEthernet 0/1, the following is displayed after you run the **show interface gigabitEthernet 0/1** command:

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

Examples

The following example sets the interval of load calculation for the interface GigabitEthernet 0/1 to 180s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# load-interval 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 logging

Function

Run the **logging** command to configure interface information printing.

Run the **no** form of this command to delete the interface information printing configuration.
The interface information printing function is disabled by default.

Syntax

logging [**link**-**updown** | **error**-**frame** | **link**-**dither** | **res**-**lack**-**frame** | **crc**-**frame**]

no logging [**link**-**updown** | **error**-**frame** | **link**-**dither** | **res**-**lack**-**frame** | **crc**-**frame**]

Parameter Description

link-updown: Prints the information when the interface state changes.

error-frame: Prints the information when the interface receives error frames.

link-dither: Prints the information when the interface flaps.

res-lack-frame: Prints the information when the interface drops the received frames due to insufficient resources.

crc-frame: Prints the notification displayed when the interface receives cyclic redundancy check (CRC) error packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can decide whether to enable interface information printing. The function is enabled by default. Notifications displayed when the interface state changes, the interface receives an error frame or flaps, the interface drops the received frame due to insufficient resources, and the interface receives a CRC error packet will be printed. The notifications will not be printed after you run the **no logging** [**link**-**updown** | **error**-**frame** | **link**-**dither** | **res**-**lack**-**frame** | **crc**-**frame**] command.

Examples

The following example prints the interface state change information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# logging link-updown
```

Notifications

When the interface state changes, the following notification will be displayed:

```
%LINK-UPDOWN: Interface GigabitEthernet 0/0, changed state to up.
%LINEPROTO-UPDOWN: Line protocol on Interface GigabitEthernet 0/0, changed state to
up.
```

When the interface receives error frames, the following notification will be displayed:

```
%PORT-ERR_FRAME: Received error frames on interface GigabitEthernet 0/0. Please check
the physical link.
```

When the interface flaps, the following notification will be displayed:

```
%LINK-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.
%LINK-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be shutdown.Please check the physical link
```

When the interface drops the received frames due to insufficient resources, the following notification will be displayed:

```
% PORT-DROP_FRAME: No more ingress buffer frames has been detected on interface GigabitEthernet 0/1. (no buffer frames: 10)
```

When the interface receives CRC error packets, the following notification will be displayed:

```
%PORT-CRC_FRAME: Detected CRC alignment errors on interface TenGigabitEthernet 1/0/7. (crc frames: 15)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 mtu

Function

Run the **mtu** command to configure the maximum transmission unit (MTU) of an interface.

By default, the MTU of an interface is 1500 bytes.

Syntax

mtu *mtu-value*

Parameter Description

mtu-value: MTU value, in bytes. The value range is related to the interface type, for example, the MTU value of a 1000 Mb port ranges from 64 to 9216.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the MTU of an interface, that is, the maximum length of a data frame at the link layer.

When the interface is configured with the default MTU, it will also be displayed using the **show run** command. After being configured, the valid MTU of the interface does not change with the MTU configuration of the system.

The set MTU may affect the throughput and delay of the network. Moreover, the set MTU generally depends on the service application and bandwidth size. If multiple services are used in a mixed manner, one service, for example, voice transmission, may impose a high requirement on real-time performance and features a small data length, while another service, for example, FTP data transmission, has no requirement on real-time performance but features a large data length, which occupies more bandwidth resources. In this case, setting a smaller MTU is conducive to the average allocation of bandwidth among different service data.

This command will cause a problem to the RSR30 series products. The on-board Gigabit Ethernet interface of the RSR30 series products does not count the data not exceeding 1518 bytes as super long frames. Therefore, when the configured MTU value is less than 1518 bytes, the interface cannot count the Ethernet frame of the Ethernet packet with a length greater than that of MTU but less than 1518 bytes as a super long frame (the interface packet on the CLI command line is counted as giant type).

Examples

The following example sets the MTU of the interface GigabitEthernet 0/1 to 9000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mtu 9000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 mtu forwarding

Function

Run the **mtu forwarding** command to configure the forwarding plane MTU.

The default value of the forwarding plane MTU is 1500 bytes.

Syntax

mtu forwarding *number*

Parameter Description

number: Forwarding plane MTU, in bytes. The value range is from 64 to 9216.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command only takes effect on all the physical ports.

After the command is configured, the protocol plane MTU will be inconsistent with the forwarding plane MTU, which may cause problems such as flow interruption and protocol exception in some scenarios. For example, in the IPv6 scenario, if the global **mtu forwarding** configuration is smaller than the default MTU configured for the interface, the IPv6 packet cannot be sent and received normally, and the network will be interrupted. You are advised to use the **system mtu** command instead of this command unless there are special scenario requirements.

Examples

The following example sets the forwarding plane MTU to 9000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mtu forwarding 9000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 negotiation mode

Function

Run the **negotiation mode** command to configure the interface auto negotiation mode.

Run the **no** form of this command to restore the default configuration.

The auto negotiation mode is disabled by default.

Syntax

negotiation mode { **on** | **off** }

no negotiation mode

Parameter Description

on: Enables the auto negotiation mode.

off: Disables the auto negotiation mode.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The auto negotiation state of an interface is not completely equivalent to the auto negotiation mode. The auto negotiation state of an interface is jointly determined by the interface rate, duplex mode, flow control mode, and auto negotiation mode.

Examples

The following example enables the auto negotiation mode for the interface GigabitEthernet 1/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# negotiation mode on
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 physical-port dither protect

Function

Run the **physical**-**port dither protect** command to configure port flapping protection.

Run the **no** form of this command to disable port flapping protection.

The port flapping protection function is enabled by default.

Syntax

physical-**port dither protect**

no physical-port dither protect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can decide whether to enable the flapping protection function for the port link. The flapping protection function is enabled by default, that is, the **physical-port dither protect** command is configured. When the port flaps for more than the specified times, the port is shut down for port protection. After the **no physical-port dither protect** command is configured, only the notification is displayed, and the port will not be shut down.

The command detects flapping every 2s or 10s. If it is detected that the port flaps six times within 2s, the system displays a notification. The port is shut down after the notification is displayed for consecutive ten times (that is, port flapping is detected continuously within 20s). If flapping is detected every 10s and flapping occurs for more than consecutive ten times, a notification is displayed but the port is not shut down.

Examples

The following example disables the port flapping protection function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no physical-port dither protect
```

Notifications

When it is detected that the port flaps six times every 2s or flaps ten times within 10s, the following notification will be displayed:

```
%LINK-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.
```

When the port flaps ten times within 20s and the last flapping occurs, the following notification will be displayed:

```
%LINK-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be shutdown.Please check the physical link.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 port speed-mode

Function

Run the **port speed-mode** command to configure the working rate mode of the 25 Gbps port.

The port works in 25 Gbps rate mode by default.

Syntax

port speed-mode { **25G** | **10G** }

Parameter Description

25G: Indicates that the 25 Gbps port works in the 25 Gbps rate mode.

10G: Indicates that the 25 Gbps port works in the 10 Gbps rate mode.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Only the 25 Gbps port supports this command. The four consecutive 25 Gbps ports in the same slot need to be configured to work in the same rate mode.

Only the 25 Gbps ports with the same rate mode are allowed to join the same aggregation group.

Running the **default interface** command does not clear the port speed-mode configuration on the 25 Gbps port.

Examples

The following example sets the rate mode of the interface TFGigabitEthernet 0/1 to 10 Gbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface TFGigabitEthernet 0/1
Hostname(config-if-TFGigabitEthernet 0/1)# port speed-mode 10G
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 protected-ports route-deny

Function

Run the **protected-ports route-deny** command to configure L3 routing blocking between protected ports.

The L3 routing blocking function between protected ports is disabled by default.

Syntax

protected-ports route-deny

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the L3 routing between protected ports is not blocked. In this case, you can run the **protected-ports route-deny** command to block the routing between protected ports.

Examples

The following example configures L3 routing blocking between protected ports.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# protected-ports route-deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 show interfaces

Function

Run the **show interfaces** command to view the details of an interface.

Syntax

show interfaces [*interface-type interface-number*] [**description** [**up** | **down**] | **switchport** | **trunk**]

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the details of all interfaces are displayed.

description: Interface description, including the link status.

up: Displays the statistics of the interface in **Up** state.

down: Displays the statistics of the interface in **Down** state.

switchport: L2 interface information. This parameter is effective only for a L2 interface.

trunk: Trunk port information. This parameter is effective for a physical port or an AP.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command without any parameter can be used to display the basic interface information.

The support to parameters varies for the L2 and L3 interfaces. The actual support conditions of specific interfaces prevail.

Examples

The following example displays the interface information of GigabitEthernet 0/1 in trunk mode.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN, line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia
00d0.f865.de9b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
```

```
  Admin speed is AUTO, oper speed is Unknown
  Flow receive control admin status is OFF,flow send control admin status is OFF
  Flow receive control oper status is Unknown,flow send control oper status is Unknown
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
  Port-type: trunk
  Native vlan:1
  Allowed vlan lists:1-4094
  Active vlan lists:1, 3-4
Queueing strategy: FIFO
  Output queue 0/0, 0 drops;
  Input queue 0/75, 0 drops
Rxload is 1/255,Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

Table 1-1 Output Fields of the show interface Command

Field	Description
Index	Indicates the interface index information, including the decimal and hexadecimal formats.
GigabitEthernet/line protocol	Indicates the interface link status/protocol status information.
Hardware	Indicates the interface hardware type.
address	Indicates the MAC address of the interface.
Interface address	Indicates the IP address of the interface.
ARP type	Indicates the ARP type.
ARP Timeout	Indicates the ARP timeout.
Interface IPv6 address	Indicates the IPv6 address of the interface.
MTU	Indicates the MTU of the interface.
BW	Indicates the interface bandwidth.
Encapsulation protocol	Indicates the interface encapsulation protocol.
loopback	Indicates whether loopback is set for the interface.
Keepalive interval	Indicates the keepalive packet sending interval of the interface.

Field	Description
Carrier delay	Indicates the carrier delay of the interface, in seconds.
Medium-type	Indicates the interface medium type.
Last link state change time	Indicates the time when the interface is up/down last time.
Time duration since last link state change	Indicates the duration of the interface status.
Priority	Indicates the interface priority.
Admin duplex mode/oper duplex	Indicates the duplex mode/operational duplex status of the interface.
Admin speed/oper speed	Indicates the rate mode/operational rate status of the interface.
Flow control admin/oper status	Indicates the flow control mode/operational flow control status of the interface.
Queuing strategy	Indicates the queuing strategy of the interface.
Output/Input/drops	Indicates the quantities of packets received/sent/dropped by the interface.
Rxload/Txload	Indicates the load rate of packets received/sent by the interface.
5 minutes input rate bit/sec packets/sec	Indicates the packet receiving rate of the interface, in bits/sec and packets/sec.
5 minutes output rate bit/sec packets/sec	Indicates the packet sending rate of the interface, in bits/sec and packets/sec.
packets input, bytes, no buffer	Indicates the statistics of the packets received by the interface and the error packets.
Received broadcasts, runts, giants	Indicates the statistics of the broadcast/multicast packets received by the interface, small packets dropped, and large packets dropped.
input errors, CRC, frame, overrun, abort	Indicates the statistics of packet receiving errors of the interface.
packets output, bytes, underruns	Indicates the statistics of packets sent by the interface, and processing failures due to fast transmission.
output errors, collisions, interface resets	Indicates the statistics of packet sending errors of the interface, retransmission times due to collisions, and interface resetting times.

The following example displays the interface information of GigabitEthernet 0/1 in access mode.

```
Hostname> enable
```

```
Hostname# show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN, line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia
00d0.f865.de9b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: access
    Vlan id : 2
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255, Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

The following example displays the interface information of GigabitEthernet 0/1 in hybrid mode.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN, line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
```

```
 MTU 1500 bytes, BW 1000000 Kbit
 Encapsulation protocol is Ethernet-II, loopback not set
 Keepalive interval is 10 sec , set
 Carrier delay is 2 sec
 Ethernet attributes:
   Last link state change time: 2012-12-22 14:00:48
   Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
   Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
   Priority is 0
   Medium-type is Copper
   Admin duplex mode is AUTO, oper duplex is Unknown
   Admin speed is AUTO, oper speed is Unknown
   Flow receive control admin status is OFF,flow send control admin status is OFF
   Flow receive control oper status is Unknown,flow send control oper status is Unknown
   Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
 Bridge attributes:
   Port-type: hybrid
   Tagged vlan id:2
   Untagged vlan id:none
 Queueing strategy: FIFO
   Output queue 0/0, 0 drops;
   Input queue 0/75, 0 drops
 Rxload is 1/255 ,Txload is 1/255
 5 minutes input rate 0 bits/sec, 0 packets/sec
 5 minutes output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer, 0 dropped
   Received 0 broadcasts, 0 runts, 0 giants
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
   0 packets output, 0 bytes, 0 underruns , 0 dropped
   0 output errors, 0 collisions, 0 interface resets
```

The following example displays the L2 information of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1 switchport
Interface              Switchport Mode     Access Native Protected VLAN lists
GigabitEthernet 0/1     enabled    ACCESS    2     1     Disabled  ALL
```

Figure 1-1 Output Fields of the show interface switchport Command

Field	Description
Interface	Indicates the interface name.
Switchport Mode	Indicates whether the switching mode is set.
Access	Indicates that the VLAN is accessed
Native	Indicates the native VLAN.

Protected	Indicates whether interface protection is enabled.
VLAN lists	Indicates the VLAN list.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show interfaces counters

Function

Run the **show interfaces counters** command to view the statistics of packets received and sent by an interface.

Syntax

show interfaces [*interface-type interface-number*] **counters** [**increment** | **errors** | **rate** | **summary**] [**up** | **down**] [**nozero**]

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.

increment: Displays the statistics of packets added in the previous sampling interval.

errors: Displays the statistics of error packets.

drops: Displays the statistics of dropped packets.

rate: Displays the packet sending/receiving rate of the interface.

summary: Displays a summary of interface packets.

up: Displays the statistics of the interface in **Up** state.

down: Displays the statistics of the interface in **Down** state.

nozero: Displays the statistics of the interface with some statistical values of interface packet quantity not equal to 0.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the packet statistics of all the interfaces are displayed.

Examples

The following example displays the statistics of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1 counters
Interface : GigabitEthernet 0/1
5 minute input rate: 9144 bits/sec, 9 packets/sec
5 minute output rate: 1280 bits/sec, 1 packets/sec
Rxload             : 1%
InOctets           : 17310045
InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts         : 100
InMulticastPkts     : 100
InBroadcastPkts     : 800
Txload             : 1%
OutOctets          : 1282535
OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts        : 100
OutMulticastPkts    : 100
OutBroadcastPkts    : 800
Undersize packets   : 0
Oversize packets    : 0
collisions         : 0
Fragments          : 0
Jabbers            : 0
CRC alignment errors : 0
AlignmentErrors     : 0
FCSErrors          : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264
  65-127: 47427
  128-255: 3478
  256-511: 658
  512-1023: 18016
  1024-1518: 125
Packet increment in last sampling interval(5 seconds):
  InOctets           : 10000
  InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts         : 100
  InMulticastPkts     : 100
  InBroadcastPkts     : 800
  OutOctets          : 10000
  OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
```

```
OutUcastPkts        : 100
OutMulticastPkts    : 100
```

Table 1-2 Output Fields of the show interfaces counters Command

Field	Description
Interface	Indicates the interface name.
5 minute input rate: bits/sec, packets/sec	Indicates the interface packet receiving rate.
5 minute output rate: bits/sec, packets/sec	Indicates the interface packet sending rate.
Rxload	Indicates the receiving bandwidth usage.
InOctets	Indicates the number of bytes in received packets.
InPkts	Indicates the sum of the received unicast, multicast, and broadcast packets. The percentages of unicast, multicast, and broadcast packets are in the brackets.
InUcastPkts	Indicates the number of unicast packets received by the interface.
InMulticastPkts	Indicates the number of multicast packets received by the interface.
InBroadcastPkts	Indicates the number of broadcast packets received by the interface.
Txload	Indicates the transmission bandwidth usage.
OutOctets	Indicates the number of bytes of total packets sent by the interface.
OutPkts	Indicates the sum of the sent unicast, multicast, and broadcast packets. The percentages of unicast, multicast, and broadcast packets are in the brackets.
OutUcastPkts	Indicates the number of unicast packets sent by the interface.
OutMulticastPkts	Indicates the number of multicast packets sent by the interface.
OutBroadcastPkts	Indicates the number of broadcast packets sent by the interface.
Undersize packets	Indicates the number of packets in the correct format and with a length less than 64 bytes.
Oversize packets	Indicates the number of packets in the correct format and with a length greater than the actually configured MTU value.
collisions	Indicates the number of packets in collision during transmission.
Fragments	Indicates the number of packets with a length less than 64 bytes and with CRC or alignment errors.

Field	Description
Jabbers	Indicates the number of packets with a length greater than 1518 bytes and with CRC or alignment errors.
CRC alignment errors	Indicates the number of received packets with CRC errors.
AlignmentErrors	Indicates the number of received packets with alignment errors.
FCSErrors	Indicates the number of received packets with FCS errors.
dropped packet events	Indicates the number of packet loss events of the interface.
packets received of length	Indicates the length of the received packets.
Packet increment in last sampling interval(5 seconds)	Indicates the incremental statistics of the packets in the previous sampling interval (5 seconds).
InOctets	Indicates the number of received bytes.
InPkts	Indicates the number of received packets.
InUcastPkts	Indicates the number of received unicast packets.
InMulticastPkts	Indicates the number of received multicast packets.
InBroadcastPkts	Indicates the number of received broadcast packets.
OutOctets	Indicates the number of sent bytes.
OutPkts	Indicates the number of sent packets.
OutUcastPkts	Indicates the number of sent unicast packets.
OutMulticastPkts	Indicates the number of sent multicast packets.

The following example displays the incremental statistics of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1 counters increment
Interface : GigabitEthernet 0/1
Packet increment in last sampling interval(5 seconds):
  InOctets           : 10000
  InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts         : 100
  InMulticastPkts     : 100
  InBroadcastPkts     : 800
  OutOctets          : 10000
  OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts        : 100
  OutMulticastPkts    : 100
```

The following example displays the statistics of the error packets on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1 counters errors
Interface    UnderSize          OverSize           Collisions         Fragments
Gi0/1       0                 0                 0                 0
Interface    Jabbers            CRC-Align-Err       Align-Err          FCS-Err
Gi0/1       0                 0                 0                 0
```

The following example displays the packet sending/receiving rate information on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interface gigabitEthernet 0/1 counters rate
Interface    Sampling Time        Input Rate          Input Rate          Output Rate
Output Rate
                              (bits/sec)          (packets/sec)       (bits/sec)
(packets/sec)
---- ------- ----------------------------
Gi0/1       5 seconds           23391              23                124
0
```

The following example displays the summary of the packets on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interface gigabitEthernet 0/1 counters summary
Interface     InOctets           InUcastPkts         InMulticastPkts
InBroadcastPkts
Gi0/1        1475788005         1389               45880503           11886621
Interface     OutOctets          OutUcastPkts        OutMulticastPkts
OutBroadcastPkts
Gi0/1        6667915            6382               31629              13410
```

The following example displays the statistics of the dropped packets on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interface gigabitEthernet 0/1 counters drops
Interface : GigabitEthernet 0/1
 Input dropped packets                : 2453
 Input no buffer packets              : 0
 Input qos dropped packets            : 0
 Output dropped packets               : 0
 Output no buffer packets             : 0
 Forwarding entry dropped packets       : 2453
```

Table 1-3 Output Fields of the show interfaces counters drops Command

Field	Description
Input dropped	Indicates the number of received packets that are dropped, excluding the packets dropped due to QoS restrictions or insufficient resources.
Input no buffer	Indicates the number of received packets that are dropped due to insufficient resources.

Field	Description
Input qos dropped	Indicates the number of received packets that are dropped due to QoS receiving restrictions.
Output dropped packets	Indicates the number of packets dropped during transmission.
Output no buffer	Indicates the number of packets that cannot be sent successfully due to lack of resources.
Forwarding entry dropped	Indicates the total number of packets dropped during forwarding, including packets dropped at the ingress and egress. Some products may not support this field. The calculation formula is: Number of packets dropped at the ingress + Number of packets dropped at the egress - Number of no buffer packets at the ingress - Number of no buffer packets at the egress - Number of CRC error packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show interfaces counters rate physical-layer

Function

Run the **show interfaces counters rate physical-layer** command to view the packet receiving and sending rate information of an interface at the physical layer.

Syntax

show interfaces [*interface-type interface-number*] **counters rate physical-layer** [**up** | **down**] [**nozero**]

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.

up: Displays the statistics of the interface in **Up** state.

down: Displays the statistics of the interface in **Down** state.

nozero: Displays the statistics of the interface with some statistical values not equal to 0.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the packet sending and receiving rate information of all the interfaces at the physical layer are displayed.

Examples

The following example displays the packet sending and receiving rate information of the interface GigabitEthernet 0/1 at the physical layer.

```
Hostname> enable
Hostname# show interface GigabitEthernet 0/1 counters rate physical-layer
Interface    Sampling Time        Input Rate          Input Rate          Output Rate
Output Rate
                              (bits/sec)          (packets/sec)       (bits/sec)
(packets/sec)
Te0/1       5 seconds           655557576             301267            655557132
```

Table 1-4 Output Fields of the show interface usage Command

Field	Description
Interface	Indicates the interface name.
Sampling Time	Specifies the interface packet sampling time.
Input Rate(bits/sec)	Specifies the physical layer packet receiving rate of the interface.
Input Rate(packets/sec)	Specifies the physical layer packet receiving rate of the interface.
Output Rate(bits/sec)	Specifies the physical layer packet sending rate of the interface.
Output Rate(packets/sec)	Specifies the physical layer packet sending rate of the interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show interfaces link-state-change statistics

Function

Run the **show interfaces link-state-change statistics** command to view the change time and count of the interface link state.

Syntax

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the details of all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the link state change information of all the interfaces are displayed.

Examples

The following example displays the link state change information of an interface.

```
Hostname> enable
Hostname# show int link-state-change statistics
Interface   Link state  Link state change times   Last change time    Link-dither
begin   Link-dither end
---- ------------ -------  -------  -----
Te0/1       down       0     2018-05-05 11:07:45  none              none
```

Table 1-5 Output Fields of show int link-state-change statistics Command

Field	Description
Interface	Indicates the interface name.
Link state	Indicates the current link state of the interface.
Link state change times	Indicates the link state change times of the interface. You can run the **clear link-state-change statistics** *interface-type interface-number* command to clear it.
Last change time	Indicates the last link state change time of the interface.

Field	Description
Link-dither begin	Indicates the start time of the last detected frequent link flapping. The value **none** indicates that no frequent link flapping occurs.
Link-dither end	Indicates the end time of the last detected frequent link flapping. The value **none** indicates that no frequent link flapping occurs. Condition of frequent link flapping: the link of the port flaps six times in 2s (the same as the condition of port flapping protection). After frequent port flapping (six times in 2s) is detected, the detection time is recorded as the start time of frequent flapping (**Link-dither begin**), and the detection continues in 2s. If no frequent port flapping is detected in 2s, or after the port is shut down by flapping protection, the detection time is recorded as the end time of frequent flapping (**Link-dither end**).

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show interfaces mtu forwarding

Function

Run the **show interfaces mtu forwarding** command to view information about the forwarding plane MTU.

Syntax

show interfaces [*interface-type interface-number*] **mtu forwarding**

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the state information of all the interfaces are displayed.

The IP MTU of L2 interface is displayed as **NA**.

Examples

The following example displays the information about the forwarding plane MTU of the interface GigabitEthernet 1/1/1.

```
Hostname> enable
Hostname# show interface GigabitEthernet 0/1 mtu forwarding
Interface                   Mtu    IP Mtu
GigabitEthernet 0/1         1500   NA
```

Table 1-6 Output Fields of the show interface mtu forwarding Command

Field	Description
Interface	Indicates the interface name.
Mtu	Indicates the MTU of the interface.
IP Mtu	For the forwarding plane MTU of the interface, the IP MTU of L2 interface is displayed as **NA**.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 show interfaces status

Function

Run the **show interfaces status** command to view the status information of an interface.

Syntax

show interfaces [*interface-type interface-number*] **status**

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the details of all interfaces are displayed.

status: Displays status information of the interface, including the rate and duplex mode.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the state information of all the interfaces is displayed.

Examples

The following example displays the status information of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interfaces GigabitEthernet 0/1 status
Interface                          Status    Vlan   Duplex   Speed     Type
---------------------------------------- --------  ----   -------  ---------- ------
GigabitEthernet 0/1                  up       1     Full     1000M     copper
```

Table 1-7 Output Fields of the show interface status Command

Field	Description
Interface	Indicates the interface name.
Status	Indicates the interface link status.
Vlan	Indicates the VLAN ID of the interface.
Duplex	Indicates the duplex mode.
Speed	Indicates the interface rate.
Type	Indicates the interface medium type.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.31 show interfaces status err-disabled

Function

Run the **show interfaces status err-disabled** command to view the errdisable status information of an interface.

Syntax

show interfaces [*interface-type interface-number*] **status err-disabled**

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the port errdisable status information of all the interfaces is displayed.

Examples

The following example displays the port errdisable status information of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show interface gigabitEthernet 0/1 status err-disabled
Interface                      Status          Reason
GigabitEthernet 0/1            err-disabled    BPDU Guard
```

Table 1-8 Output Fields of the show interface status err-disabled Command

Field	Description
Interface	Indicates the interface name.
Status	Indicates the errdisable status; **err-disable** is displayed in the case of a violation; otherwise no content is displayed.
Reason	Indicates the reason for the violation; no content is displayed if there is no violation.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.32 show interfaces transceiver

Function

Run the **show interfaces transceiver** command to view the optical module information of an interface.

Syntax

show interfaces [*interface-type interface-number*] **transceiver** [**alarm** | **diagnosis**]

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the details of all interfaces are displayed.

transceiver: Displays the basic information of the optical module.

alarm: Displays the current fault alarms of the optical module. If no fault occurs, **None** is displayed.

diagnosis: Displays the current measurement value of the diagnostic parameter of the optical module.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command without any parameter can be used to display the optical module information of all the interfaces.

Examples

The following example displays the optical module information of the 10 Gigabit interface tenGigabitEthernet 0/49.

```
Hostname> enable
Hostname# show interfaces tenGigabitEthernet 0/49 transceiver
Transceiver Type    :  10GBASE-SR-SFP+
Connector Type      :  LC
Wavelength(nm)      :  850
Transfer Distance   :
   50/125 um OM2 fiber
      -- 300m
   62.5/125 um OM1 fiber
      -- 300m
Digital Diagnostic Monitoring  : YES
Vendor Serial Number          : M1102232386

Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)   Voltage(V)      Bias(mA)           RX power(dBm)       TX power(dBm)
43(OK)          3.27(OK)        6.24(OK)           -3.92(OK)[AP]       -1.90(OK)

Transceiver current alarm information:
None
```

Table 1-9 Output Fields of the show interface transceiver Command

Field	Description
Transceiver Type	Indicates the type of the transmit end.
Connector Type	Indicates the type of the connector.
Wavelength(nm)	Indicates the optical wavelength.
Digital Diagnostic Monitoring	Indicates self-diagnosis monitoring.
Vendor Serial Number	Indicates serial number of the vendor.

The following example displays the current fault alarms of the optical module of the 10 Gigabit interface tenGigabitEthernet 0/49.

```
Hostname> enable
Hostname# show interfaces tenGigabitEthernet 0/49 transceiver alarm
tengigabitEthernet 0/49 transceiver current alarm information:
RX loss of signal
```

Table 1-10 Output Fields of the show interface transceiver alarm Command

Field	Description
RX loss	Indicates loss of received packets.

The following example displays the current measurement value of the diagnostic parameter of the optical module for the 10 Gigabit interface tenGigabitethernet 0/49.

```
Hostname> enable
Hostname# show interfaces tenGigabitEthernet 0/49 transceiver diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)   Voltage(V)     Bias(mA)          RX power(dBm)      TX power(dBm)
38(OK)         3.20(OK)       0.04(OK)          -40.00(alarm)[AP]  -40.00(alarm)
```

Table 1-11 Output Fields of the show interface transceiver diagnosis Command

Field	Description
Temp(Celsius)	Indicates the temperature.
Voltage(V)	Indicates the voltage.
Bias(mA)	Indicates the current.
RX power(dBm)	Indicates the receive power.
TX power(dBm)	Indicates the transmit power.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.33 show interfaces usage

Function

Run the **show interfaces usage** command to view the bandwidth usage of an interface.

Syntax

show interfaces [*interface-type interface-number*] **usage** [**up** | **down**]

Parameter Description

interface-type interface-number: Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.

up: Displays the bandwidth usage of the interface in **Up** state.

down: Displays the bandwidth usage of the interface in **Down** state.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface name is specified, the bandwidth usage information of all the interfaces is displayed. The bandwidth here refers to the actual link bandwidth rather than the configured bandwidth value on the interface.

The support to parameters varies for the L2 and L3 interfaces. The actual support conditions of specific interfaces prevail.

Examples

The following example displays the bandwidth usage information of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Interface                Bandwidth    Average Usage     Output Usage    Input
Usage
GigabitEthernet 0/0        1000 Mbit    0.002822759%      0.001183280%
0.004462237%
```

Table 1-12 Output Fields of the show interface usage Command

Field	Description
Interface	Indicates the interface name.
Bandwidth	Indicates the bandwidth of the interface link, that is, the maximum rate of the link.
Average Usage	Indicates the current bandwidth usage.
Input Usage	Indicates the receiving bandwidth usage.
Output Usage	Indicates the transmission bandwidth usage.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.34 show mgmt virtual

Function

Run the **show mgmt virtual** command to view the information of the virtual management port.

Syntax

show mgmt virtual

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information of the virtual management port.

```
Hostname> enable
```

```
Hostname# show mgmt virtual
Mgmt 0
Virtual MGMT Member:
   1/M1/MGMT0: Active
```

Table 1-13 Output Fields of the show mgmt virtual Command

Field	Description
Virtual MGMT Member	Indicates the members of the management port.
1/M1/MGMT0	Indicates the management port 0.
Active	Indicates the active status of the management port.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.35 show split summary

Function

Run the **show split summary** command to view the splitting/combining information of an interface.

Syntax

show split summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to view the splitting/combining information of all the splittable interfaces.

Examples

The following example displays the splitting/combining information of an interface.

```
Hostname> enable
```

```
Hostname# show split summary
Port         SpliteStatus SplitPorts
Hu1/1        merged      Hu1/1:1    Hu1/1:2    Hu1/1:3    Hu1/1:4
Hu1/2        merged      Hu1/2:1    Hu1/2:2    Hu1/2:3    Hu1/2:4
Hu1/3        merged      Hu1/3:1    Hu1/3:2    Hu1/3:3    Hu1/3:4
Hu1/4        merged      Hu1/4:1    Hu1/4:2    Hu1/4:3    Hu1/4:4
Hu1/5        merged      Hu1/5:1    Hu1/5:2    Hu1/5:3    Hu1/5:4
Hu1/6        merged      Hu1/6:1    Hu1/6:2    Hu1/6:3    Hu1/6:4
Hu1/7        merged      Hu1/7:1    Hu1/7:2    Hu1/7:3    Hu1/7:4
Hu1/8        merged      Hu1/8:1    Hu1/8:2    Hu1/8:3    Hu1/8:4
Hu3/25       merged      Hu3/25:1   Hu3/25:2   Hu3/25:3   Hu3/25:4
Hu3/26       merged      Hu3/26:1   Hu3/26:2   Hu3/26:3   Hu3/26:4
```

Table 1-14 Output Fields of the show split summary Command

Field	Description
Port	Indicates the main interface splittable.
SpliteStatus	Indicates the current splitting/combining status.
SplitPorts	Indicates the member interfaces after the splittable interface is split.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.36 shutdown

Function

Run the **shutdown** command to shut down a specific interface.

Run the **no** form of this command to enable the interface.

The interface is in **Up** state by default.

Syntax

shutdown

no shutdown

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the command to shut down interfaces (including Ethernet ports, APs, and SVIs). Other configurations of the interfaces still exists, but does not work. You can run the **show interfaces** command to view the interface status.

Running this command on an interface means disabling the interface. On the synchronous serial interface, the DTR and RTS will be directly set to invalid. If the external modem is provided with a DTR or RTS signal indicator, the indicator will be turned off. The indicator at the synchronous interface of the device will also go out.

Note

To prevent unwanted link flapping caused by frequent operation of the **shutdown/no shutdown** command, there should be a certain time interval (which must be greater than the carrier delay of the interface) before/after configuring the **shutdown**/**no shutdown** command twice on an interface.

Examples

The following example shuts down the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Related Commands

N/A

1.37 snmp trap link-status

Function

Run the **snmp trap link-status** command to enable the LinkTrap notification sending function for interface status change.

Run the **no** form of this command to restore the default configuration.

The LinkTrap notification sending function for interface status changes is enabled by default.

Syntax

snmp trap link-status

no snmp trap link-status

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the command to configure the link trap sending function for the interfaces (including Ethernet ports, APs, and SVIs). When the function is enabled, the SNMP module sends link traps if the link status changes on the interface.

Examples

The following example disables the LinkTrap notification sending function on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 snmp-server if-index persist

Function

Run the **snmp-server if-index persist** command to enable the interface index persistence function.

The interface index persistence function is disabled by default.

Syntax

snmp-server if-index persist

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the **snmp-server if-index persist** command is executed, the indexes of all the current interfaces are saved during configuration saving, and the indexes remain unchanged after the device is restarted.

Examples

The following example enables the interface index persistence function. In other words, the interface index remains unchanged after the device is restarted.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server if-index persist
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 speed

Function

Run the **speed** command to configure the rate of an interface.

Run the **no** form of this command to restore the default configuration.

The interface rate is adaptive by default.

Syntax

speed [**10** | **100** | **1000** | **10G** | **40G** | **auto**]

no speed

Parameter Description

10: The interface rate of 10 Mbps.

100: The interface rate of 100 Mbps.

1000: The interface rate of 1000 Mbps.

10G: The interface rate of 10 Gbps.

40G: The interface rate of 40 Gbps.

Auto: Indicates that the rate of the interface is adaptive.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If an interface is an AP member port, the rate of this interface is determined by the rate of the AP. When the interface exits the AP, it uses its own rate configuration. You can run the **show interfaces** command to view the rate configuration. The rate options available to an interface vary with the type of the interface. For example, you cannot set the rate of a small form-factor pluggable (SFP) interface to 10 Mbps.

You need to set **duplex** in addition to **speed** when using the interface auto-negotiation function, that is, the duplex mode and 10/100 Mbps rate adaptation. The following table describes usage of the **duplex** and **speed** commands.

Table 1-15 Correspondence between duplex and rate

duplex	speed	Work Mode
Full	10	Forced to work in 10M full duplex mode.
Full	100	Forced to work in 100M full duplex mode.
Half	10	Forced to work in 10M full duplex mode.
Half	100	Forced to work in 100M full duplex mode.
Auto	auto	The Ethernet interface works in adaptive mode.

Examples

The following example sets the rate of the interface GigabitEthernet 0/1 to 100 Mbps.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# speed 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 split interface

Function

Run the **split interface** command to configure the interface splitting function.

Run the **no** form of this command to delete the interface splitting configuration.

The interface is in combined status by default.

Syntax

split interface FortyGigabitEthernet *interface-number*

no split interface FortyGigabitEthernet *interface-number*

Parameter Description

interface-number: Interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example splits the 40 Gbps interface FortyGigabitEthernet 0/1 into four 10 Gbps interfaces.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# split interface FortyGigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 statistics

Function

Run the **statistics** command to enable the interface traffic statistics collection and IP traffic statistics collection functions.

Run the **no** form of this command to disable the interface traffic statistics collection and IP traffic statistics collection functions.

The IP traffic statistics collection function is disabled for all the interfaces by default.

Syntax

statistics { **enable** | **ip enable** }

no statistics { **enable** | **ip enable** }

Parameter Description

enable: Enables the interface traffic statistics collection function.

ip enable: Enables the IP traffic statistics collection function of the interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the **show interface** *port-name* command to view the statistical results, and the **clear counter** command to clear the statistics.

The interface traffic statistics collection and IP traffic statistics collection functions can be enabled for the virtual interfaces such as sub-interfaces and SVIs. The IP traffic statistics collection function can be enabled for the Ethernet interface and Ethernet AP.

Support for interface statistics collection varies with different products. For example, only the IP traffic statistics collection function can be enabled for some products.

The **statistics enable** and **route-sample enable** commands have the same function. The **show running-config** command is used to display all the configurations.

If the **ip-sample enable** command has been configured, when the **statistics enable** command is configured, the configuration made by **ip-sample enable** is automatically cleared first, the interface IP traffic statistics collection function is disabled, and the interface traffic statistics collection function is still enabled.

If the **ip-sample enable** command has been configured, when the **statistics ip enable** command is configured, the configuration made by **ip-sample enable** will be automatically cleared first, the interface traffic statistics collection function is disabled, and the interface IP traffic statistics collection function is still enabled.

Examples

The following example enables the IP traffic statistics collection function for an Ethernet interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# statistics ip enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 switchport

Function

Run the **switchport** command to configure the L2 mode for an interface.

Run the **no** form of this command to configure the L3 mode for an interface.

All the interface are in the L2 mode by default.

Syntax

switchport

no switchport

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command takes effect only for the interfaces associated with physical ports. The **switchport** command shuts down the interface and then restarts it, during which the device sends a message indicating the connection status. If an interface is switched from L2 mode to L3 mode, all the L2 attributes of the interface are deleted.

Examples

The following example configures the L3 mode for the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no switchport
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 switchport protected

Function

Run the **switchport protected** command to configure a port as protected port.

A protected port is not configured for the port by default.

Syntax

switchport protected

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the ports on the device need to be isolated from each other, these ports can be set as protected ports. In this case, only the L2 communication is blocked, and the L3 route is still accessible. You can run the global command **protected-ports route-deny** to block the L3 route.

Examples

The following example configures the port GigabitEthernet 0/1 as protected port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport protected
```

Notifications

N/A

Common Errors

N/A

Platform Description

This command is not supported on the AP of the CB line card.

Related Commands

N/A

1.44 system mtu

Function

Run the **system mtu** command to configure the MTU of the system.

The MTU of the system is not configured by default.

Syntax

system mtu *mtu-value*

Parameter Description

mtu-value: MTU value, in bytes. The value range is related to the interface type, for example, the value range for a 1000 Mbps port is from 64 to 9216. The default value is 1500.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Configuring the MTU of the system will update the MTU effective values of all the Ethernet interfaces (including the APs) of the system. However, if the interface is configured with an MTU, the MTU configured for the interface will take effect.

Examples

The following example sets the system MTU to 9000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# system mtu 9000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Aggregate Port Commands

Command	Function
aggregate bfd-detect	Enable the bidirectional forwarding detection (BFD) function of an aggregate port (AP) member port.
aggregateport algorithm mode	Configure the load balancing algorithm mode for all APs.
aggregateport capacity mode	Configure the capacity mode of an AP.
aggregateport load-balance	Configure the global load balancing algorithm of APs or the load balancing algorithm of a specified AP.
aggregateport member linktrap	Enable the LinkTrap notification sending function of member ports of an AP.
aggregateport member minimum	Configure the minimum number of member ports of an AP or the action to be triggered when the number of member ports of an AP is less than the minimum number.
aggregateport primary-port	Configure a member port of an AP as a preferred port.
clear lacp counters	Clear the Link Aggregation Control Protocol (LACP) packet statistics from an LACP AP member port.
debug lacp	Enable the LACP debugging function.
hash-disturb	Configure a load balancing hash disturbance factor.
hash-symmetrical	Configure the load balancing hash synchronization factor.
interface aggregateport	Configure the Ethernet AP or enter the interface configuration mode of Ethernet AP.
ipv4 field	Configure the load balancing mode of IPv4 packets in the specified enhanced load balancing profile.
ipv6 field	Configure the load balancing mode of IPv6 packets in the specified enhanced load balancing profile.
l2 field	Configure the load balancing mode of L2 packets in the specified enhanced load balancing profile.
lacp device	Configure the device ID of LACP.

lacp individual-port enable	Enable the LCAP independent port function.
lacp individual-timeout period	Configure the timeout period of an LACP independent port.
lacp port-priority	Configure the port priority of an LACP AP member port.
lacp short-timeout	Configure the timeout mode of an LACP AP member port to the short timeout mode.
lacp short-timeout period	Configure the timeout period of the LACP system in short timeout mode.
lacp system-id	Configure the LACP system ID.
lacp system-priority	Configure the LACP system priority.
load-balance-profile	Rename the enhanced load balancing profile and enter the enhanced load balancing profile mode.
port-group	Configure an Ethernet physical port as a member port of a static AP.
show aggregateport load-balance	View the global load balancing information of an AP.
show aggregateport summary	Display the configuration of an AP.
show aggregateport capacity	Display the capacity mode and capacity usage of the current AP.
show lacp counters	Display the packet statistics of an LACP AP member port.
show lacp summary	Display the state of an LACP AP.
show load-balance-profile	Display the configuration of the enhanced load balancing mode.

1.1 aggregate bfd-detect

Function

Run the **aggregate bfd-detect** command to enable the bidirectional forwarding detection (BFD) function of an aggregate port (AP) member port.

Run the **no** form of this command to disable the BFD function of an AP member port.

The BFD function of an AP member port is disabled by default.

Syntax

aggregate bfd-detect { **ipv4** *source-ipv4-address destination-ipv4-address* | **ipv6** *source-ipv6-address destination-ipv6-address* }

no aggregate bfd-detect { **ipv4** | **ipv6** }

Parameter Description

ipv4: Enables IPv4 BFD. You can enable IPv4 BFD when the IPv4 address is used on the AP.

Ipv6: Enables IPv6 BFD. You can enable IPv6 BFD when the IPv6 address is used on the AP.

source-ipv4-address: Source IPv4 address, that is, the IP address configured on the AP.

destination-ipv4-address: Destination IPv4 address, that is, the IP address configured on the peer AP.

source-ipv6-address: Source IPv6 address, that is, the IP address configured on the AP.

destination-ipv6-address: Destination IPv6 address, that is, the IP address configured on the peer AP.

Command Modes

AP interface configuration mode

Default Level

14

Usage Guidelines

To enable the BFD function of an AP member port, you need to configure BFD parameters. For details, see “BFD” in “Configuring Reliability”.

When a device supports both IPv4 BFD and IPv6 BFD, IPv4 BFD and IPv6 BFD can be enabled at the same time on the AP.

Note

After the BFD function is enabled for the link aggregation group on the AP, BFD sessions are automatically set up on the member ports in forwarding state in the AP.

Examples

The following example enables the BFD function for the member ports of AP1, and configures the local IP address for BFD as 1.0.0.1, the remote IP address as 1.0.0.2, the minimum sending interval as 50 milliseconds, the minimum receiving interval as 50 milliseconds, and the detection timeout multiplier as 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregateport 1
Hostname(config-if-Aggregateport 1)# ip address 1.0.0.1
Hostname(config-if-Aggregateport 1)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
Hostname(config-if-Aggregateport 1)# bfd interval 50 min_rx 50 multiplier 3
```

Notifications

When the source IP address or destination IP address is invalid, the following notification will be displayed:

```
% Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 aggregateport algorithm mode

Function

Run the **aggregateport algorithm mode** command to configure the load balancing algorithm mode for all APs.

Run the **no** form of this command to restore the default value of the load balancing algorithm mode for all APs.

The type number of the algorithm mode is 11 by default.

Syntax

aggregateport algorithm mode *algorithm-number*

no aggregateport algorithm mode

Parameter Description

algorithm-number: Type number of the algorithm mode. The value ranges from 3 to 11.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

(Optional) This command is configured when the load balancing algorithm mode needs to be changed.

You can run the **no aggregateport algorithm mode** command to restore the default algorithm mode.

Examples

The following example sets the load balancing algorithm mode to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aggregateport algorithm mode 3
```

Notifications

When the algorithm mode fails to be configured, the following notification will be displayed:

```
Set algorithm mode failed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 aggregateport capacity mode

Function

Run the **aggregateport capacity mode** command to configure the capacity mode of an AP.

Run the **no** form of this command to restore the default value of the capacity mode of an AP.

By default, the maximum number of an AP is 128, and the maximum number of member ports per aggregateport is 8.

Syntax

aggregateport capacity mode *capacity-mode*

no aggregateport capacity mode

Parameter Description

capacity-mode: Capacity mode to be configured. The supported capacity mode is 128*8.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the capacity mode configuration is supported, the system provides several configurable capacity modes for users.

Examples

The following example sets the maximum number of APs to 128, and the maximum number of member ports of an AP to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aggregateport capacity mode 128*8
```

Notifications

When the existing maximum AP number of the current system exceeds the maximum number of APs to be configured, the following notification will be displayed:

```
% Set aggregateport capacity mode failed.aggregateport 129 have been created, cannot set maximum aggregateport number to128.
```

When the current number of member ports in AP 1 exceeds the maximum number of member ports to be configured, the following notification will be displayed:

```
% Set aggregateport capacity mode failed. current aggregateport member count of aggregateport 1 more than 9.
```

When the link aggregation capacity mode has been configured and you need to save the configuration and restart the system to enable the configuration, the following notification will be displayed:

```
% Warning: please save configuration and restart the device for the configuration to take effect!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 aggregateport load-balance

Function

Run the **aggregateport load-balance** command to configure the global load balancing algorithm of APs or the load balancing algorithm of a specified AP.

Run the **no** form of this command to restore the default value of the global load balancing algorithm of APs or restore the load balancing algorithm of a specified AP to the global load balancing algorithm.

By default, for a device on which an AP is created as a L2 AP by default, load is distributed according to the source MAC addresses and destination MAC addresses of the incoming packets. For a device on which an AP is created as a L3 AP by default, load is distributed according to the source IP addresses and destination IP addresses of the incoming packets. For the device that is provided with a CB type line card and supports the enhanced load balancing mode, the AP sets the corresponding packet type field according to the enhanced load balancing profile to distribute load.

Syntax

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **enhanced profile** *profile-name*

no aggregateport load-balance

Parameter Description

dst-mac: Indicates that load is distributed according to the destination MAC addresses of incoming packets. On each link of the AP, packets with the same destination MAC address are sent to the same port, and packets with different destination MAC addresses are distributed to different ports.

src-mac: Indicates that load is distributed according to the source MAC addresses of the incoming packets. On each link of the AP, packets with different source MAC addresses are distributed to different ports, and packets with the same source MAC address use the same port.

src-dst-ip: Indicates that the load is distributed according to the source IP address and destination IP address. Packets with different source IP addresses and destination IP addresses are forwarded through different ports. Packets with the same source IP address and destination IP address are forwarded through the same link. You are advised to adopt this load balancing mode under L3 conditions.

dst-ip: Indicates that load is distributed according to the destination IP addresses of the incoming packets. On each link of the AP, packets with the same destination IP address are sent to the same port, and packets with different destination IP addresses are distributed to different ports.

src-ip: Indicates that load is distributed according to the source IP addresses of the incoming packets. On each link of the AP, packets with different source IP addresses are distributed to different ports, and packets with the same source IP address use the same port.

src-dst-mac: Indicates that load is distributed according to the source MAC addresses and destination MAC addresses. Packets with different source MAC addresses and destination MAC addresses are forwarded through different ports. Packets with the same source MAC address and destination MAC address are forwarded through the same link.

src-dst-ip-l4port: Indicates that load is distributed according to the source IP address and the destination IP address, as well as the source L4 port number and the destination L4 port number.

enhanced profile *profile-name*: Configures the corresponding packet type field according to **profile-name** to distribute load.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

The load balancing algorithm is configured in the interface configuration mode of the specified AP. After the configuration takes effect, the newly configured load balancing algorithm will operate on the AP. You `can use the **no aggregateport load-balance** command in the interface configuration mode of the AP to disable the load balancing algorithm configured on this AP. After that, the global load balancing algorithm configured on the current device for link aggregation takes effect.

Examples

The following example configures a destination MAC address-based load balancing algorithm for link aggregation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aggregateport load-balance dst-mac
```

The following example configures a destination MAC address-based load balancing algorithm on AP 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregateport 1
Hostname(config-if-AggregatePort 1)# aggregateport load-balance dst-mac
```

Notifications

N/A

Common Errors

N/A

Platform Description

Specification

The **src-dst-ip-l4port** and **src-dst-ip-src-dst-l4port** commands both indicate the load balancing mode based on the source and destination IP addresses and L4 source and destination port numbers of packets. The **src-dst-ip-l4port** command is applicable to all the products supporting this load balancing mode, while the **src-dst-ip-src-dst-l4port** command is applicable only to some products.

Related Commands

N/A

1.5 aggregateport member linktrap

Function

Run the **aggregateport member linktrap** command to enable the LinkTrap notification sending function of member ports of an AP.

Run the **no** form of this command to disable the LinkTrap notification sending function of member ports of an AP.

The LinkTrap notification sending function of member ports of an AP is disabled by default.

Syntax

aggregateport member linktrap

no aggregateport member linktrap

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In interface configuration mode, you cannot use the [**no**] **snmp trap link-status** command to enable or disable the LinkTrap notification sending function of member ports of an AP. Instead, in global configuration mode, you can use the [**no**] **aggregateport member linktrap** command to enable this function.

Examples

The following example enables the LinkTrap notification sending function of member ports of an AP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aggregateport member linktrap
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 aggregateport member minimum

Function

Run the **aggregateport member minimum** command to configure the minimum number of member ports of an AP or the action to be triggered when the number of member ports of an AP is less than the minimum number.

Run the **no** form of this command to delete the minimum number of member ports of an AP or the action to be triggered when the number of member ports of an AP is less than the minimum number.

By default, the minimum number of member ports of an AP is 1, and no action is configured.

Syntax

aggregateport member minimum { *port-number* | **action shutdown** }

no aggregateport member minimum [**action**]

Parameter Description

port-number: Minimum number of member ports. The value range is from 1 to 8.

shutdown: Indicates that the AP will be shut down if the number of member ports of an AP is less than the minimum number.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

(Optional) This command is configured to specify the minimum number of the member ports of an aggregation group.

For a static AP, the same configuration is required for the peer end; otherwise it may cause the local AP to be **Down** and the peer AP to be **Up**.

Examples

The following example sets the minimum number of member ports of AP 1 to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregatePort 1
Hostname(config-if-AggregatePort 1)# aggregateport member minimum 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 aggregateport primary-port

Function

Run the **aggregateport primary-port** command to configure a member port of an AP as a preferred port.

Run the **no** form of this command to restore the default value of the preferred member port of an AP.

No preferred port is configured by default.

Syntax

aggregateport primary-port

no aggregateport primary-port

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Only one preferred port can be configured for one AP.

Examples

The following example configures the member port GigabitEthernet 0/1 of AP 1 as the preferred port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# port-group 1 mode active
Hostname(config-if-GigabitEthernet 0/1)# aggregateport primary-port
```

Notifications

When a non-member port is configured as the preferred port, the following notification will be displayed:

```
% The interface gigabitEthernet 0/1 is not aggregateport member.
```

When more than two preferred ports are configured for one AP, the following notification will be displayed:

```
% Already specified gigabitEthernet 0/1 as primary port for aggregateport 1
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 clear lacp counters

Function

Run the **clear lacp counters** command to clear the Link Aggregation Control Protocol (LACP) packet statistics from an LACP AP member port.

Syntax

clear lacp counters [*key-number* | *interface-type interface-number*]

Parameter Description

key-name: Number of the specified LACP AP. The value range is from 1 to 128.

interface-type interface-number: Interface type and interface number of the specified LACP AP member port.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can run the **show lacp counters** command in privileged EXEC mode to view the LACP packet statistics, and run the **clear lacp counters** command in privileged EXEC mode to clear the LACP packet statistics. You can specify the interface number of a specific member port or AP. If no interface is specified, the LACP packet statistics of all the LACP AP member ports will be cleared.

Examples

The following example clears the LACP packet statistics of the member port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname# clear lacp counters GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 debug lacp

Function

Run the **debug lacp** command to enable the LACP debugging function.

Run the **no** form of this command to disable the LACP debugging function.

The debugging function is enabled by default.

Syntax

debug lacp { **cache-database** | **cli** | **ef-packet** | **thread** | **pkt-agent** | **pkt-statis** | **pkt-thread** | **packet** | **event** | **ha** | **realtime** | **stm** | **timer** | **all** }

no debug lacp { **cache-database** | **cli** | **ef-packet** | **thread** | **pkt-agent** | **pkt-statis** | **pkt-thread** | **packet** | **event** | **ha** | **realtime** | **stm** | **timer** | **all** }

Parameter Description

cache-database: Database operation debugging.

cli: Command processing debugging.

ef-packet: LACP packet linkage path debugging.

thread: Process scheduling debugging.

pkt-agent: Agent thread packet debugging.

pkt-statis: Packet statistics debugging.

pkt-thread: Agent thread scheduling debugging.

packet: LACP packet sending and receiving debugging.

event: LACP event processing debugging.

ha: Master-slave backup processing debugging.

realtime: Debugging information record file.

stm: State machine debugging.

timer: Internal timer debugging.

all: Enables all LACP debugging.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the LACP packet sending and receiving debugging functions.

```
Hostname> enable
Hostname# configure terminal
Hostname# debug lacp packet
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 hash-disturb

Function

Run the **hash-disturb** command to configure a load balancing hash disturbance factor.

Run the **no** form of this command to disable the load balancing hash disturbance function.

The load balancing hash disturbance function is disabled by default.

Syntax

hash-disturb *factor-string*

no hash-disturb

Parameter Description

factor-string: Disturbance factor.

Command Modes

Enhanced load balancing profile configuration mode

Default Level

14

Usage Guidelines

(Optional) You can run this command when an AP needs to be specified for multiple devices of the same type to balance packets of the same type, and run the **no hash-disturb** command to disable the hash disturbance function.

It is not guaranteed that either configuration affects the balancing effect. If there is no expected effect, the other value can be configured.

Examples

The following example configures hash disturbance factor A.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile
Hostname(config-load-balance-profile)# hash-disturb A
```

Notifications

When the hash disturbance factor fails to be configured, the following notification will be displayed:

```
% Set hash-disturb failed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 hash-symmetrical

Function

Run the **hash-symmetrical** command to configure the load balancing hash synchronization factor.

Run the **no** form of this command to disable the load balancing hash synchronization function.

The load balancing hash synchronization factor is not configured by default.

Syntax

hash-symmetrical { **ipv4** | **ipv6** }

no hash-symmetrical { **ipv4** | **ipv6** }

Parameter Description

ipv4: Indicates that the load balancing hash synchronization function is enabled for IPv4 packets.

ipv6: Indicates that the load balancing hash synchronization function is enabled for IPv6 packets.

Command Modes

Enhanced load balancing profile configuration mode

Default Level

14

Usage Guidelines

You can run the **hash-symmetrical** { **ipv4** | **ipv6** } command to enable the hash synchronization function when the same path needs to be specified for the uplink and downlink streams of a certain packet type..

Examples

The following example disables the hash synchronization function for IPv6 packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile
Hostname(config-load-balance-profile)# no hash-symmetrical ipv6
```

Notifications

When the balancing hash synchronization function for IPv4 packets fails to be enabled, the following notification will be displayed:

```
% Set hash-symmetrical ipv4 failed.
```

When the balancing hash synchronization function for IPv6 packets fails to be enabled, the following notification will be displayed:

```
% Set hash-symmetrical ipv6 failed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 interface aggregateport

Function

Run the **interface aggregateport** command to configure the Ethernet AP or enter the interface configuration mode of Ethernet AP.

Run the **no** form of this command to delete an Ethernet AP.

No AP is configured by default.

Syntax

interface aggregateport *ap-number*

no interface aggregateport *ap-number*

Parameter Description

ap-number: Number of an AP. The value ranges from 1 to 128,.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If an AP has been created, the system automatically enters the interface configuration mode of the AP when the **interface aggregateport** command is configured. If no AP is created, an AP will be created first when the **interface aggregateport** command is configured. If the AP is created successfully, the system will enter the interface configuration mode of the AP.

Examples

The following example creates AP 1 and enters its interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interfaces aggregateport 1
Hostname(config-if-Aggregateport 1)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv4 field

Function

Run the **ipv4 field** command to configure the load balancing mode of IPv4 packets in the specified enhanced load balancing profile.

Run the **no** form of this command to restore the default configuration.

The load balancing mode of IPv4 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

Syntax

ipv4 field [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**] [**dst-port**]

no ipv4 field

Parameter Description

src-ip: Indicates that the load is distributed according to the source IP addresses of incoming IPv4 packets.

dst-ip: Indicates that the load is distributed according to the destination IP addresses of incoming IPv4 packets.

protocol: Indicates that the load is distributed according to the protocol types of incoming IPv4 packets.

l4-src-port: Indicates that the load is distributed according to the L4 source port numbers of incoming IPv4 packets.

l4-dst-port: Indicates that the load is distributed according to the L4 destination port numbers of incoming IPv4 packets.

src-port: Indicates that the load is distributed according to the source port numbers of incoming IPv4 packets.

Command Modes

Enhanced load balancing profile configuration mode

Default Level

14

Usage Guidelines

You need to create an enhanced load balancing profile before running this command.

Examples

The following example sets the load balancing mode of IPv4 packets in the enhanced load balancing profile APL to **src-ip**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile apl
Hostname(config-load-balance-profile)# ipv4 field src-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 field

Function

Run the **ipv6 field** command to configure the load balancing mode of IPv6 packets in the specified enhanced load balancing profile.

Run the **no** form of this command to restore the default configuration.

The load balancing mode of IPv6 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

Syntax

ipv6 field [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**]

no ipv6 field

Parameter Description

src-ip: Indicates that the load is distributed according to the source IP addresses of incoming IPv6 packets.

dst-ip: Indicates that the load is distributed according to the destination IP addresses of incoming IPv6 packets.

protocol: Indicates that the load is distributed according to the protocol types of incoming IPv6 packets.

l4-src-port: Indicates that the load is distributed according to the L4 source port numbers of incoming IPv6 packets.

l4-dst-port: Indicates that the load is distributed according to the L4 destination port numbers of incoming IPv6 packets.

src-port: Indicates that the load is distributed according to the source port numbers of incoming IPv6 packets.

Command Modes

Enhanced load balancing profile configuration mode

Default Level

14

Usage Guidelines

You need to create an enhanced load balancing profile before running this command.

Examples

The following example sets the load balancing mode of IPv6 packets in the enhanced load balancing profile APL to **src-ip**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile apl
Hostname(config-load-balance-profile)# ipv6 field src-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 l2 field

Function

Run the **l2 field** command to configure the load balancing mode of L2 packets in the specified enhanced load balancing profile.

Run the **no** form of this command to restore the default configuration.

The load balancing mode of L2 packets is a combination of **src-mac** and **dst-mac** by default.

Syntax

l2 field [**src-mac**] [**dst-mac**] [**src-port**]

no l2 field

Parameter Description

src-mac: Indicates that the load is distributed according to the source MAC addresses of incoming L2 packets.

dst-mac: Indicates that the load is distributed according to the destination MAC addresses of incoming L2 packets.

src-port: Indicates that the load is distributed according to the source port numbers of incoming L2 packets.

Command Modes

Enhanced load balancing profile configuration mode

Default Level

14

Usage Guidelines

You need to create an enhanced load balancing profile before running this command.

Examples

The following example sets the load balancing mode of L2 packets to **src-mac** and **src-port**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile apl
Hostname(config-load-balance-profile)# l2 field src-mac src-port
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 lacp device

Function

Run the **lacp device** command to configure the device ID of LACP.

Run the **no** form of this command to cancel the configured device ID.

The device ID is 0 by default.

Syntax

lacp device *device-id*

no lacp device

Parameter Description

device-id: Device ID of LACP. The value range is from 0 to 3.

Command Modes

AP interface configuration mode

Default Level

14

Usage Guidelines

(Optional) You can run this command when the LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

This command must be used together with the **lacp system-id** command

Examples

The following example sets the device ID of AP 1 to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregatePort 1
Hostname(config-if-AggregatePort 1)# lacp device 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 lacp individual-port enable

Function

Run the **lacp individual-port enable** command to enable the LCAP independent port function.

Run the **no** form of this command to restore the default configuration.

The LACP independent port function is disabled by default.

Syntax

lacp individual-port enable

no lacp individual-port enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

(Optional) You can run this command to convert an LACP AP member port to a common physical port when the LACP AP member port cannot perform LACP negotiation.

This command is used to enable the independent port function. After the function is enabled, when a member port fails to receive the LACP packet sent by the peer end within the timeout period of the independent port and the negotiation fails, the member port enters the independent port state (that is, is converted to a common physical port).

Examples

The following example enables GigabitEthernet 0/1 as an independent port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# port-group 1 mode active
Hostname(config-if-GigabitEthernet 0/1)# lacp individual-port enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 lacp individual-timeout period

Function

Run the **lacp individual-timeout period** command to configure the timeout period of an LACP independent port.

Run the **no** form of this command to restore the default configuration.

The timeout period of an LACP independent port is 90s by default.

Syntax

lacp individual-timeout period *time*

no lacp individual-timeout period

Parameter Description

time: Timeout period of the independent port, in seconds. The value range is from 10 to 90.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

(Optional) You can run this command to adjust the timeout period of an independent port for the LACP independent port function.

This command is used to configure the timeout period for the independent port function. Its configuration affects only ports with the LACP independent port function enabled.

Configuring the timeout period of an independent port will not affect existing independent ports.

A member port that fails to receive the LACP packet sent by the peer end within the timeout period of an independent port enters the independent port state (that is, is converted to a common physical port).

In long timeout mode, the LACP packet is sent every 30s. The timeout period should be longer than 30s so as not to affect the normal LACP negotiation. You are advised to configure the timeout period at least twice the period of LACP packet sending. In short timeout mode, the timeout period is not limited.

Examples

The following example sets the timeout period of an independent port to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lacp individual-timeout period 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 lacp port-priority

Function

Run the **lacp port-priority** command to configure the port priority of an LACP AP member port.

Run the **no** form of this command to restore the port priority of the LACP AP member port.

The priority of the LACP AP member port is 32768 by default.

Syntax

lacp port-priority *Priority*

no lacp port-priority

Parameter Description

Priority: LACP port priority of the port. The value range is from 0 to 65535. A smaller value indicates a higher priority.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the LACP port priority of GigabitEthernet 0/1 to 4096.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lacp port-priority 4096
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 lacp short-timeout

Function

Run the **lacp short-timeout** command to configure the timeout mode of an LACP AP member port to the short timeout mode.

Run the **no** form of this command to restore the timeout mode of the LACP AP member port to the long timeout mode.

The timeout mode of an LACP AP member port is long timeout by default.

Syntax

lacp short-timeout

no lacp short-timeout

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In long timeout mode, the port sends an LACP packet every 30 seconds, and a timeout occurs if no packet is received within 90 seconds.

In short timeout mode, the port sends an LACP packet every 1 second, and a timeout occurs if no packet is received within 3 seconds.

Examples

The following example configures the LACP port timeout mode of GigabitEthernet 0/1 to the short timeout mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lacp short-timeout
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 lacp short-timeout period

Function

Run the **lacp short-timeout period** command to configure the timeout period of the LACP system in short timeout mode.

Run the **no** form of this command to restore the default configuration.

The timeout period of the LACP system in short timeout mode is 3 seconds by default.

Syntax

lacp short-timeout period *interval*

no lacp short-timeout period

Parameter Description

interval: Timeout period in short timeout mode, in seconds. The value ranges from 3 to 90.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to configure the timeout period in short timeout mode.

Examples

The following example sets the timeout period of the LACP system in short timeout mode to 4 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lacp short-timeout period 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 lacp system-id

Function

Run the **lacp system-id** command to configure the LACP system ID.

Run the **no** form of this command to restore the default LACP system ID.

The LACP system ID is the system ID (MAC address) of the device by default.

Syntax

lacp system-id *system-id*

no lacp system-id

Parameter Description

system-id: LACP system ID of the port, a valid unicast MAC address.

Command Modes

AP interface configuration mode

Default Level

14

Usage Guidelines

(Optional) You can run this command when the LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

The command must be used together with the **lacp device** command.

Examples

The following example sets the LACP system ID to 0000.1236.54ab.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface aggregatePort 1
Hostname(config-if-AggregatePort 1)#lacp system-id 0000.1236.54ab
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 lacp system-priority

Function

Run the **lacp system-priority** command to configure the LACP system priority.

Run the **no** form of this command to restore the LACP system priority.

The LACP system priority of a port is 32768 by default.

Syntax

lacp system-priority *system-priority*

no lacp system-priority

Parameter Description

system-priority: LACP system priority of a port. The value range is from 0 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the LACP system priority to 4096.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lacp system-priority 4096
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 load-balance-profile

Function

Run the **load-balance-profile** command to rename the enhanced load balancing profile and enter the enhanced load balancing profile mode.

Run the **default** form of this command to restore the current profile to the default load balancing configuration, with the profile name unchanged.

The name of the enhanced load balancing profile is **default** by default.

Syntax

load-balance-profile *profile-name*

default load-balance-profile *profile-name*

Parameter Description

profile-name: Profile name, which includes a maximum of 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the device is configured with an enhanced load balancing profile named **default**, which cannot be configured or deleted. You can directly enter the default enhanced load balancing profile mode using the **load-balance-profile default** command, or rename the enhanced load balancing profile using the **load-balance-profile** *profile-name* command.

Examples

The following example creates and enters an enhanced load balancing profile named APL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# load-balance-profile apl
Hostname(config-load-balance-profile)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 port-group

Function

Run the **port-group** command to configure an Ethernet physical port as a member port of a static AP.

Run the **port-group mode** command to configure a physical port as a member port of an LACP AP.

Run the **no** form of this command to delete the AP member attribute of the port.

By default, the Ethernet physical port does not belong to any static AP or LACP AP.

Syntax

port-group *port-group-number*

port-group *key-number* **mode** { **active** | **passive** }

no port-group

Parameter Description

port-group-number: Number of the member port group of the static AP, that is, the interface number of the static AP. The value ranges from 1 to 128.

key-number: Number of the member port group of the LACP AP, that is, the interface number of the LACP AP. The value ranges from 1 to 128.

active: Indicates that the port will initiate LACP aggregation operation.

passive: Indicates that the port will not actively initiate LACP aggregation operation, but will passively participate in LACP aggregation operation after receiving LACP packets from a neighbor.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When you run the **port-group** command to add a port to an AP, if the AP does not exist, it will be automatically created. When the layer of the physical port is different from that of the AP, the physical port cannot be added to the AP.

Examples

The following example configures GigabitEthernet 0/1 as a member port of static AP 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# port-group 1
```

The following example configures GigabitEthernet 0/1 as a member port of LACP AP 1 and sets the aggregation mode to active mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# port-group 1 mode active
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show aggregateport load-balance

Function

Run the **show aggregateport load-balance** command to view the global load balancing information of an AP.

Syntax

show aggregateport load-balance

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of global load-balance.

```
Hostname> enable
Hostname# show aggregateport load-balance
Load-balance    : Source MAC and Destination MAC
Algorithm mode
 current: 11, default: 11
```

Table 1-1 Output Fields of the show aggregateport load-balance Command

Field	Description
Load-balance	Indicates the global load balancing mode.
Algorithm mode	Hash balancing algorithm mode: ● **current**: Indicates the current effective value. ● **default**: Indicates the default value of the device.
	●

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show aggregateport summary

Function

Run the **show aggregateport summary** command to display the configuration of an AP.

Syntax

show aggregateport [*aggregate-port-number*] **summary**

Parameter Description

aggregate-port-number:-port-number: Number of the AP. The value range is from 1 to 128. If the port number is not specified, the information of all APs will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface number of an AP is specified, the information of all APs will be displayed.

If the system does not support configuring the load balancing mode based on AP, the **Load-balance** field will not be displayed.

Examples

The following example displays the configuration of AP 1.

```
Hostname> enable
Hostname# show aggregateport 1 summary
AggregatePort  MaxPorts       SwitchPort Mode    Load balance              Ports
Ag1          8             Enabled    ACCESS  dst-mac                   Gi0/1
```

Table 1-2 Output Fields of the show aggregateport summary Command

Field	Description
AggregatePort	Indicates the interface name of the AP.
MaxPorts	Indicates the maximum number of ports that can be supported in an AP.
SwitchPort	Indicates whether the AP is a L2 port. **Enabled** indicates that it is a L2 port, and **Disabled** indicates that it is not a L2 port.
Mode	Indicates L2 port attributes of the AP, including **ACCESS**, **TRUNK**, **TUNNEL**, **HYBRID**,

Field	Description
	UPLINK, **HOST**, and **PROMIS**. When the AP is not a L2 port, the field is blank.
Load balance	Indicates the load balancing mode of the AP.
Ports	Indicates the name of the AP member port.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show aggregateport capacity

Function

Run the **show aggregateport capacity** command to display the capacity mode and capacity usage of the current AP.

Syntax

show aggregateport capacity

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the capacity mode and capacity usage of the current AP.

```
Hostname> enable
Hostname# show aggregateport capacity
AggregatePort Capacity Information:
```

```
Configuration Capacity Mode: 128*8.
Effective Capacity Mode    : 128*8.
Available Capacity         : 128*8.
Total Number: 128, Used: 1, Available: 127.
```

Table 1-3 Output Fields of the show aggregateport capacity Command

Field	Description
Configuration Capacity Mode	Indicates the currently configured capacity mode
Effective Capacity Mode	Indicates the currently effective capacity mode.
Available Capacity	Indicates the currently available capacity mode.
Total Number	Indicates the maximum number of available APs in the current system. **Used** indicates the number of used APs, and **Available** indicates the number of remaining available APs.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show lacp counters

Function

Run the **show lacp counters** command to display the packet statistics of an LACP AP member port.

Syntax

show lacp counters [*key-number*]

Parameter Description

key- number: Number of the specified LACP AP. The value range is from 1 to 128. If the port number is not specified, the information of all ports will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If **key-number** is not specified, the LACP packet statistics of all the LACP AP member ports will be displayed.

Examples

The following example displays the LACP packet statistics of member ports of LACP AP 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# show lacp counters 1
LACP PDU Pakcet Statistics
Aggregate port 1:
Port        InPkts    OutPkts
Gi0/1        6121     6132
```

Table 1-4 Output Fields of the show lacp counters Command

Field	Description
Aggregate port 2	Indicates the AP ID.
Port	Indicates the LACP AP member port name.
InPkts	Indicates the number of LACP PDU packets received by the member port.
OutPkts	Indicates the number of LACP PDU packets sent by the member port.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 show lacp summary

Function

Run the **show lacp summary** command to display the state of an LACP AP.

Syntax

show lacp summary [*key-number*]

Parameter Description

key-number: Number of a specified LACP AP. The value range is from 1 to 128. If the port number is not specified, the information of all LACP APs will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If **key-number** is not specified, the state information of all LACP APs will be displayed.

Examples

The following example displays the state information of LACP AP 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# show lacp summary 1
System Id:32768,00d0.f8fb.0002
Flags:  S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.
Aggregate port 1:
Local information:
LACP port      Oper    Port    Port
Port    Flags    State    Priority       Key    Number  State
Gi0/1    SA       bndl       4096        0x3    0x1     0x3d
Gi0/2    SA       bndl       4096        0x3    0x2     0x3d
Gi0/3    SA       bndl       4096        0x3    0x3     0x3d
Partner information:
LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number   State
Gi0/1    SA       61440    00d0.f800.0002   0x3    0x1    0x3d
Gi0/2    SA       61440    00d0.f800.0002   0x3    0x2    0x3d
Gi0/3    SA       61440    00d0.f800.0002   0x3    0x3    0x3d
```

Table 1-5 Output Fields of the show lacp summary Command

Field	Description
System Id	Indicates the system ID, namely, the system MAC address.
Aggregate port 1	Indicates the name of the AP.
Local information	Indicates the information about the local LACP AP member port.
Port	Indicates the LACP AP member port name.

Field	Description
Flags	Indicates the configuration of member ports. For details, see the description of SFAP in the displayed notification.
State	Indicates the member port negotiation state: **bndl** indicates successful negotiation, **susp** indicates negotiation failure, and **down** indicates the **Down** state of the port link.
LACP port Priority	Indicates the port priority of the LACP AP member port.
Oper Key	Indicates the aggregation group number of the LACP AP member port.
Port Number	Indicates the number of the LACP AP member port.
Port State	Indicates the port state details of the LACP AP member port.
Partner information	Indicates the information about the peer LACP AP member port.
Port	Indicates the name of the local port connected to the peer end.
Flags	Indicates the configuration of the peer LACP AP member port, which is the same as the above **Flags**.
LACP port Priority	Indicates the port priority of the peer LACP AP member port, which is the same as the above **LACP port Priority**.
Dev ID	Indicates the ID of the device system where the peer LACP AP member port is, that is, the MAC address of the peer device.
Oper Key	Indicates the aggregation group number of the peer LACP AP member port, which is the same as the above **Oper Key**.
Port Number	Indicates the number of the peer LACP AP member port, which is the same as the above **Port Number**.
Port State	Indicates the port state details of the peer LACP AP member port, which is the same as the above **Port State**.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 show load-balance-profile

Function

Run the **show load-balance-profile** command to display the configuration of the enhanced load balancing mode.

Syntax

show load-balance-profile [*profile-name*]

Parameter Description

profile-name: Profile name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If *profile-name* is not specified, the information of all the enhanced load balancing profiles will be displayed.

Examples

The following example displays the enhanced load balancing configuration of the profile module0.

```
Hostname> enable
Hostname# show load-balance-profile module0
Load-balance-profile: module0
Packet   Hash Field:
     IPv4: src-ip dst-ip
    IPv6: src-ip dst-ip
    L2  : src-mac dst-mac
```

Table 1-6 Output Fields of the show load-balance-profile Command

Field	Description
Load-balance-profile	Indicates the name of the enhanced load balancing profile.
IPv4	Indicates the balancing configuration of IPv4 packets in the enhanced load balancing profile.
IPv6	Indicates the balancing configuration of IPv6 packets in the enhanced load balancing profile.
L2	Indicates the balancing configuration of L2 packets in the enhanced load balancing profile.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Ethernet Switching Commands

1. MAC Address Commands
2. MAC Loopback Commands
3. VLAN Commands
4. Private VLAN Commands
5. Super VLAN Commands
6. Voice VLAN Commands
7. GVRP Commands
8. QinQ Commands
9. MSTP Commands
10. ERPS Commands
11. LLDP Commands

1 MAC Address Commands

Command	Function
clear mac-address-table dynamic	Clear dynamic Media Access Control Address (MAC) address entries.
clear mac-address-table flapping record	Clear the MAC address flapping records.
mac-address-learning (global mode)	Enable the MAC address learning function in global configuration mode.
mac-address-learning (interface mode)	Enable the MAC address learning function in interface configuration mode.
mac-address-table aging-time	Configure the aging time for dynamic MAC address entries.
mac-address-table filtering	Configure a filtering MAC address entry for a specified VLAN.
mac-address-table notification	Enable the MAC address change notification function in global configuration mode.
mac-address-table static	Configure a static MAC address entry.
max-dynamic-mac-count	Configure the upper limit of dynamic MAC addresses learned from a VLAN or an interface.
max-dynamic-mac-count exceed-action	Set the packet forwarding rule to be used after the number of dynamic MAC addresses learned from a VLAN or an interface reaches the upper limit.
show mac-address-learning	Display the MAC address learning capability in interface configuration mode.
show mac-address-table	Display all types of MAC address entries.
show mac-address-table aging-time	Display the aging time of dynamic MAC address entries.
show mac-address-table count	Display statistics about MAC address entries in a MAC address table.
show mac-address-table dynamic	Display dynamic MAC address entries.
show mac-address-table filtering	Display filtering MAC address entries.
show mac-address-table flapping record	Display dynamic MAC address flapping records.

show mac-address-table max-dynamic-mac-count	Display the upper limit of learned dynamic MAC addresses.
show mac-address-table interface	Display static or dynamic MAC address entries for a specified interface.
show mac-address-table notification	Display MAC address change notifications.
show mac-address-table static	Display the static MAC address entries.
show mac-address-table evpn	Display the MAC address entries for an EVPN.
show mac-address-table mlag	Display the MAC address entries for an MLAG.
show mac-address-table vlan	Display all types of MAC address entries for a specified VLAN.
show mac-address-table vsi	Display all types of MAC address entries for a specified VSI.
show mac-address-table vni	Display all types of MAC address entries for a specified VNI.
show mac-address-table all	Display all types of MAC address entries.
snmp trap mac-notification	Enable the MAC address change notification function for an interface.
mac-address-table warning-interval	Configure the interval for reporting MAC address table usage alarms.
mac-address-table warning-threshold	Configure the upper and lower limits for reporting MAC address table usage alarms.
mac-address-table flapping-logging	Enable MAC address flapping detection.
mac-address-table flapping action	Enable the MAC address flapping protection policy.

1.1 clear mac-address-table dynamic

Function

Run the **clear mac-address-table dynamic** command to clear dynamic Media Access Control Address (MAC) address entries.

Syntax

clear mac-address-table dynamic [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]

Parameter Description

dynamic: Clears all dynamic MAC address entries.

address *mac-address*: Clears a specified dynamic MAC address entry.

interface *interface-type interface-number*: Clears dynamic MAC addresses on the specified interface.

vlan *vlan-id*: Clears all dynamic MAC addresses in a specified VLAN. *vlan-id*: ID of a specified virtual local area network (VLAN). The value range is from 1 to 4094.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

You can use the **show mac-address-table dynamic** command to display all information in a dynamic MAC address table.

Examples

The following example clears all dynamic MAC address entries.

```
Hostname> enable
Hostname# clear mac-address-table dynamic
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **show mac-address-table dynamic**

1.2 clear mac-address-table flapping record

Function

Run the **clear mac-address-table flapping record** command to clear the MAC address flapping records.

Syntax

clear mac-address-table flapping record

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example clears the MAC address flapping records.

```
Hostname> enable
Hostname# clear mac-address-table flapping record
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 mac-address-learning (global mode)

Function

Run the **mac-address-learning** command to enable the MAC address learning function in global configuration mode.

Run the **no** form of **mac-address-learning** command to disable the MAC address learning function in global configuration mode.

Run the **default** form of this command to restore the default configuration.

MAC address learning is enabled in global configuration mode by default.

Syntax

mac-address-learning { **enable** | **disable** }

default mac-address-learning

Parameter Description

enable: Enables the MAC address learning function in global configuration mode.

disable: Disables the MAC address learning function in global configuration mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the MAC address learning function is enabled in global configuration mode, the status of the MAC address learning function on an interface is subject to the configuration of the interface. When the MAC address learning function is disabled in global configuration mode, all interfaces do not learn MAC addresses.

Examples

The following example disables MAC address learning in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-learning disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac-address-learning (interface mode)**

1.4 mac-address-learning (interface mode)

Function

Run the **mac-address-learning** command to enable the MAC address learning function in interface configuration mode.

Run the **no** form of this command to disable the MAC address learning function in interface configuration mode.

Run the **default** form of this command to restore the default configuration.

The MAC address learning function is enabled in interface configuration mode by default.

Syntax

mac-address-learning

no mac-address-learning

default mac-address-learning

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Do not disable the MAC address learning function on an interface where the security function is enabled. If the MAC address learning function is disabled, the security function becomes unavailable on the interface.

If you run the **default interface** command in global configuration mode for an interface that includes L2 sub-interfaces, it is forbidden to restore the MAC address learning function on the interface to the default configuration.

Examples

The following example disables the MAC address learning function on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no mac-address-learning
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac-address-learning (global mode)**

1.5 mac-address-table aging-time

Function

Run the **mac-address-table aging-time** command to configure the aging time for dynamic MAC address entries.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The aging time for dynamic MAC address entries is 300 seconds by default.

Syntax

mac-address-table aging-time *time*

no mac-address-table aging-time

default mac-address-table aging-time

Parameter Description

time: Aging time of dynamic MAC address entries, in seconds. The value ranges from 10 to 1000000. The value **0** indicates no aging.

Command Modes

Global configuration mode

Default Level

14

Examples

The following example sets the aging time of dynamic MAC address entries to 400s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table aging-time 400
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show mac-address-table aging-time**

1.6 mac-address-table filtering

Function

Run the **mac-address-table filtering** command to configure a filtering MAC address entry for a specified VLAN.

Run the **no** form of this command to delete a filtering MAC address entry.

Run the **default** form of this command to delete a filtering MAC address entry.

No filtering MAC address entry is configured by default.

Syntax

mac-address-table filtering *mac-address* **vlan** *vlan-id*

no mac-address-table filtering *mac-address* **vlan** *vlan-id*

default mac-address-table filtering *mac-address* **vlan** *vlan-id*

Parameter Description

mac-address: Filtering MAC address entry.

vlan *vlan-id*: Specifies a VLAN for which MAC addresses are to be filtered out. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this function is configured, packets with the source or destination MAC address matching the MAC address in the filtering MAC address entry are discarded.

You cannot configure a multicast address as a filtering MAC address. You can use the **show mac-address-table filtering** command to display filtering MAC address settings.

Examples

The following example configures the MAC address 0000.0202.0303 as a filtering MAC address entry for VLAN 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table filtering 0000.0202.0303 vlan 3
```

Notifications

When an invalid MAC address is configured in a filtering MAC address entry, the following notification will be displayed:

```
Can not set this filter address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show mac-address-table filtering**

1.7 mac-address-table notification

Function

Run the **mac-address-table notification** command to enable the MAC address change notification function in global configuration mode.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The MAC address change notification function is disabled in global configuration mode by default.

Syntax

mac-address-table notification [**interval** *interval* | **history-size** *size*]

no mac-address-table notification [**interval** | **history-size**]

default mac-address-table notification [**interval** | **history-size**]

Parameter Description

interval *interval*: Specifies the interval for sending MAC address Trap messages. The value range is from 1 to 3600 in seconds, and the default value is **1**.

history-size *size*: Specifies the maximum number of entries in the history table for MAC address entry change notifications. The value range is from 1 to 1200, and the default value is **50**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The MAC address change notification function applies to dynamic MAC address entries and security MAC address entries only. No Trap notification is generated for static MAC address entries and filtering MAC address entries.

You can run the **snmp**-**server enable traps mac**-**notification** command in global configuration mode to send MAC address Trap messages to the Network Management Station (NMS).

Examples

The following example enables the MAC address change notification function in global configuration mode, sets the interval for sending MAC address Traps to 40s, and sets the maximum number of MAC address change notification history records to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table notification
Hostname(config)# mac-address-table notification interval 40
Hostname(config)# mac-address-table notification history-size 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **snmp-server enable traps mac-notification** (network management and monitoring/SNMP)
- **snmp-server host** (network management and monitoring/SNMP)
- **snmp trap mac-notification**

1.8 mac-address-table static

Function

Run the **mac-address-table static** command to configure a static MAC address entry.

Run the **no** form of this command to delete a static MAC address entry.

Run the **default** form of this command to delete a static MAC address entry.

No static MAC address entry is configured by default.

Syntax

mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

no mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

default mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

Parameter Description

mac-address: Destination MAC address in a static MAC address entry.

vlan *vlan-id*: Specifies a VLAN to which an egress interface belongs. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

interface *interface-type interface-number*: Specifies an egress interface for packets whose MAC address matches the static MAC address entry.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Static MAC addresses have the same function as learned dynamic MAC addresses. Compared with dynamic MAC addresses, static MAC addresses never age and they must be manually configured and deleted. Static

MAC addresses are not cleared after device reset. You can use the **show mac-address-table static** command to display static MAC address table settings.

You cannot configure a multicast address as a static MAC address.

Examples

The following example configures a static MAC address entry and sets the destination MAC address to 00e1-00e2-00e3 and the egress interface to TenGigabitEthernet 0/1 in VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address static 00e1-00e2-00e3 vlan 2 interface
TenGigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show mac-address-table static**

1.9 max-dynamic-mac-count

Function

Run the **max-dynamic-mac-count** command to configure the upper limit of dynamic MAC addresses learned from a VLAN or an interface.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

No upper limit of dynamic MAC addresses learned from a VLAN or an interface is configured by default.

Syntax

max-dynamic-mac-count *count*

no max-dynamic-mac-count

default max-dynamic-mac-count

Parameter Description

count: Upper limit of dynamic MAC addresses learned from a specified VLAN or interface. The value range is from 1 to 65535.

Command Modes

VLAN configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

After you run this command, the device will disable the MAC address learning function for the interface or VLAN if the number of dynamic MAC addresses learned from the interface or VLAN reaches the upper limit.

If the number of MAC addresses learned from the interface or VLAN is greater than the upper limit, the device will stop learning MAC addresses from the interface or VLAN and will not start learning again until the number drops below the limit as aged addresses entries are deleted.

You can run the **show mac-address-table max-dynamic-mac-count** command to display the upper limit of dynamic MAC addresses learned from the interface or VLAN and the learning result.

If you run the **default interface** command in global configuration mode for an interface that includes L2 subinterfaces, the upper limit of the MAC addresses learned from the interface cannot be restored to the default configuration.

Examples

The following example sets the upper limit of MAC addresses learned from VLAN 1 to 160.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# max-dynamic-mac-count 160
```

The following example sets the upper limit of MAC addresses learned from tenGigabitEthernet 0/1 to 160.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# max-dynamic-mac-count 160
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **max-dynamic-mac-count exceed-action**
- **show mac-address-table max-dynamic-mac-count**

1.10 max-dynamic-mac-count exceed-action

Function

Run the **max-dynamic-mac-count exceed-action** command to set the packet forwarding rule to be used after the number of dynamic MAC addresses learned from a VLAN or an interface reaches the upper limit.

Run the **no** form of this command to restore the default configuration.

By default, the device can continue forwarding packets whose source MAC address does not exist in the MAC address entries of the device when the number of learned MAC addresses reaches the upper limit.

Syntax

max-dynamic-mac-count exceed-action { *forward* | *discard* }

no max-dynamic-mac-count exceed-action { *forward* | *discard* }

Parameter Description

forward: The device can continue forwarding packets whose source MAC address does not exist in the MAC address entries of the device after the number of learned dynamic MAC addresses reaches the upper limit, without learning the source MAC address.

discard: The device discards packets whose source MAC address does not exist in the MAC address entries of the device after the number of learned dynamic MAC addresses reaches the upper limit.

Command Modes

VLAN configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

Run the command to determine whether to forward packets whose source MAC addresses are not in the MAC address table after the number of MAC addresses reaches the upper limit.

If you run the **default interface** command in global configuration mode for an interface that includes L2 subinterfaces, the packet forwarding rule applied to the interface cannot be restored to the default configuration.

Examples

The following example sets the upper limit of MAC addresses learned from VLAN 1 to 160 and enables forwarding of packets in this VLAN even when the number of MAC addresses learned from the VLAN reaches 160.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# max-dynamic-mac-count 160
Hostname(config-vlan)# max-dynamic-mac-count exceed-action forward
```

The following example sets the upper limit of MAC addresses learned from TenGigabitEthernet 0/1 to 160 and enables forwarding of packets on this interface even when the number of MAC addresses learned from the interface reaches 160.

```
Hostname> enable
Hostname#configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# max-dynamic-mac-count 160
Hostname(config-if-TenGigabitEthernet 0/1)# max-dynamic-mac-count exceed-action
forward
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **max-dynamic-mac-count**
- **show mac-address-table max-dynamic-mac-count**

1.11 show mac-address-learning

Function

Run the **show mac-address-learning** command to display the MAC address learning capability in interface configuration mode.

Syntax

show mac-address-learning

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the MAC address learning capability in interface configuration mode.

```
Hostname> enable
Hostname# show mac-address-learning
TenGigabitEthernet 0/0     learning ability: disable
TenGigabitEthernet 0/1     learning ability: enable
TenGigabitEthernet 0/2     learning ability: enable
TenGigabitEthernet 0/3     learning ability: enable
```

Table 1-1 Output Fields of the show mac-address-learning Command

Field	Description
Interface type interface number	Interface type and interface name
learning ability	MAC address learning capability in interface configuration mode: ● **enable**: The MAC address learning function of an interface is enabled and the device can learn dynamic MAC addresses from this interface. ● **disable**: The MAC address learning function of an interface is disabled and the device cannot learn dynamic MAC addresses from this interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show mac-address-table

Function

Run the **show mac-address-table** command to display all types of MAC address entries.

Syntax

show mac-address-table [**address** *mac-address*] [[**vlan** *vlan-id*] [**interface** *interface-type interface-number*] | **vsi** *vsi-id* | **vni** *vni-id*]

Parameter Description

address *mac-address*: Displays the MAC address entry of a specified MAC address.

vlan *vlan-id*: Displays the MAC address entries for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

interface *interface-type interface-number*: Displays the MAC address entries for a specified interface.

vsi-id: Displays the MAC address entries for a specified virtual switch interface (VSI). *vsi-id*: ID of the specified VSI. The value range is from 1 to 2147483647.

vni-id: Displays the MAC address entries for a specified virtual network interface (VNI). *vni-id:*-id: ID of the specified VNI. The value range is from 1 to 16777215.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

You can use this command to display all types of MAC address entries for a specified VLAN, interface, VSI, and VNI.

Examples

The following example displays the MAC address entry corresponding to the MAC address 00d0.f800.1001.

```
Hostname> enable
Hostname # show mac-address-table address 00d0.f800.1001
Vlan       MAC Address         Type     Interface            Live Time
------  ---------------- -------- ------------------- ---- -------------
1          00d0.f800.1001      STATIC  TenGigabitEthernet 0/1
```

The following example displays all MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table
Vlan       MAC Address         Type     Interface            Live Time
------  ---------------- -------- ------------------- ---- -------------
1          00d0.f800.1001      STATIC   TenGigabitEthernet 0/1  -
1          00d0.f800.1002      DYNAMIC  TenGigabitEthernet 0/1  1d 00:21:22
1          00d0.f800.1003      OTHER    TenGigabitEthernet 0/1  -
1          00d0.f800.1004      FILTER   Not available        -
```

Table 1-2 Output Fields of the show mac-address-table Command

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address ● **FILTER**: filtering MAC address ● **OTHER**: MAC address of a user authenticated via 802.1X, MAB, or Web-based authentication

Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

The following example displays the MAC address entries that contain the source MAC address 1234.2222.3333 in VSI 1.

```
Hostname> enable
Hostname# show mac-address-table address 1234.2222.3333 vsi 1
VLAN/VSI/VNI   MAC Address         Type     Learned-From           Live Time
-------------- ------------------ ------- ---------------------- -------------
-/1/-         1234.2222.3333      STATIC   TenGigabitEthernet 0/1    -
```

Table 1-3 Output Fields of the show mac-address-table vsi/vni Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address ● **FILTER**: filtering MAC address ● **OTHER**: MAC address of a user authenticated via 802.1X, MAB, or Web-based authentication
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show mac-address-table aging-time

Function

Run the **show mac-address-table aging-time** command to display the aging time of dynamic MAC address entries.

Syntax

show mac-address-table aging-time

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the aging time of dynamic MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table aging-time
Aging time    : 300
```

Table 1-4 Output Fields of the show mac-address-table aging-time Command

Field	Description
Aging time	Aging time

Notifications

N/A

Platform Description

N/A

Related Commands

- **mac-address-table aging-time**

1.14 show mac-address-table count

Function

Run the **show mac-address-table count** command to display statistics about MAC address entries in a MAC address table.

Syntax

show mac-address-table count [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Displays statistics about all MAC address entries for a specified interface.

vlan *vlan-id*: Displays statistics about all MAC address entries for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If you do not specify any parameter in this command, statistics about all MAC address entries are displayed.

Examples

The following example displays the numbers of various types of MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table count
Dynamic Address Count  : 1
EVPN   Address Count  : 0
MLAG   Address Count  : 0
Static  Address Count  : 1
Filtering Address Count: 1
Other   Address Count  : 0
Total Mac Addresses   : 3
Total Mac Address Space Available: 63997
```

The following example displays the number of MAC address entries for VLAN 1.

```
Hostname> enable
Hostname# show mac-address-table count vlan 1
Dynamic Address Count  : 7
Static  Address Count  : 0
Filter  Address Count  : 0
Other   Address Count  : 0
Total Mac Addresses   : 7
```

The following example displays the number of MAC address entries for TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac-address-table count interface tenGigabitEthernet 0/1
Dynamic Address Count  : 10
Static  Address Count  : 0
Filter  Address Count  : 0
Other   Address Count  : 0
Total Mac Addresses   : 10
```

Table 1-5 Output Fields of the show mac-address-table count Command

Field	Description
Dynamic Address Count	Number of dynamic MAC addresses
Static Address Count	Number of static MAC addresses
Filter Address Count	Number of filtering MAC addresses
Other Address Count	MAC address of a user authenticated via 802.1X, MAB, or WEB authentication
EVPN Address Count	Number of EVPN MAC addresses
MLAG Address Count	Number of MLAG MAC addresses
Total Mac Addresses	Total number of MAC addresses

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show mac-address-table dynamic

Function

Run the **show mac-address-table dynamic** command to display dynamic MAC address entries.

Syntax

show mac-address-table dynamic [**address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

address *mac-address*: Displays a specified dynamic MAC address entry.

vlan *vlan-id*: Displays all dynamic MAC addresses for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

interface *interface-type interface-number*: Displays all dynamic MAC addresses for a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If you do not specify any parameter in this command, all dynamic MAC address entries are displayed.

Examples

The following example displays all dynamic MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table dynamic
Vlan    MAC Address     Type     Interface            Live Time
------  --------------- -------- ------------------- -------------
1    0000.0000.0001     DYNAMIC  TenGigabitEthernet 0/1  1d 00:18:00
1    0001.960c.a740     DYNAMIC  TenGigabitEthernet 0/1  1d 00:21:22
1    0007.95c7.dff9     DYNAMIC  tTenGigabitEthernet 0/1  1d 00:31:30
1    0007.95cf.eee0     DYNAMIC  TenGigabitEthernet 0/1  1d 00:35:40
1    0007.95cf.f41f     DYNAMIC  TenGigabitEthernet 0/1  1d 00:48:45
1    0009.b715.d400     DYNAMIC  TenGigabitEthernet 0/1  1d 00:52:55
1    0050.bade.63c4     DYNAMIC  TenGigabitEthernet 0/1  1d 00:55:56
```

Table 1-6 Output Fields of the show mac-address-table dynamic Command

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address.
Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show mac-address-table filtering

Function

Run the **show mac-address-table filtering** command to display filtering MAC address entries.

Syntax

show mac-address-table filtering [**address** *mac-address*] [**vlan** *vlan-id* | **vni** *vni-id* | **vsi** *vsi-id*]

Parameter Description

mac-address: Specified filtering MAC address.

vlan *vlan-id*: Displays a filtering MAC address for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

vni-id: ID of a specified VNI for which filtering MAC addresses are to be displayed. The value range is from 1 to 16777215.

vsi-id: ID of a specified VSI for which filtering MAC addresses are to be displayed. The value range is from 1 to 2147483647.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the MAC address filtering table.

```
Hostname> enable
Hostname# show mac-address-table filtering
Vlan       MAC Address         Type    Interface            Live Time
---------- ------------------- ------- -------------------- -------------
1          0000.2222.2222      FILTER   Not available       -
```

Table 1-7 Output Fields of the show mac-address-table filtering Command

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address.
Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 show mac-address-table flapping record

Function

Run the **show mac-address-table flapping record** command to display dynamic MAC address flapping records.

Syntax

show mac-address-table flapping record

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

You can use the **mac-address-table flapping-logging** command to enable the MAC address flapping detection function and then use the **show mac-address-table flapping record** command to display the MAC address flapping records.

Examples

The following example displays the dynamic MAC address flapping records.

```
Hostname> enable
Hostname# show mac-address-table flapping record
 Mac address flapping detect status      : on
 Mac address flapping detect interval    : 1s
 Mac address flapping syslog supress time : 1800s
 Mac address flapping record max count   : 300
 Mac address flapping record total count  : 5
Move-Time             VLAN MAC-Address    Original-Port Move-Ports    Status
--------------------------------------------------------------------------------
 2020.11.14 12:10:46   1    0001.1111.1111 te0/2         te0/1         Normal
 2020.11.14 12:10:58   1    0001.1111.1111 te0/1         te0/2         Normal
 2020.11.14 12:11:1    1    0001.1111.1111 te0/2         te0/1         Normal
 2020.11.14 12:11:11   1    0001.1111.1111 te0/1         te0/2         Normal
 2020.11.14 12:11:13   1    0001.1111.1111 te0/2         te0/1         Normal
```

Table 1-8 Output Fields of the show mac-address-table flapping record Command

Field	Description

Field	Description
Move-Time	Specifies the time at which the dynamic MAC address flapping occurs.
VLAN	Specifies the VLAN where the dynamic MAC address flapping occurs.
MAC-Address	MAC address
Original-Port	Specifies the interface from which the dynamic MAC address is learned before MAC address flapping.
Move-Ports	Specifies the interface from which the dynamic MAC address is learned after MAC address flapping.
Status	Specifies the currently valid flapping protection policy. ● **Normal**: No flapping protection policy is set. ● **ERR-DOWN**: The interface is disabled after MAC address flapping.

Notifications

N/A

Platform Description

N/A

Related Commands

- **mac-address-table flapping-logging**

1.18 show mac-address-table max-dynamic-mac-count

Function

Run the **show mac-address-table max-dynamic-mac-count** command to display the upper limit of learned dynamic MAC addresses.

Syntax

show mac-address-table max-dynamic-mac-count { **interface** *interface-type interface-number* | **vlan** *vlan-id* }

Parameter Description

interface *interface-type interface-number*: Displays the upper limit of dynamic MAC addresses learned from a specified interface.

vlan *vlan-id*: Displays the upper limit of dynamic MAC addresses learned from a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the dynamic MAC address learning results of all VLANs for which an upper limit of learned dynamic MAC addresses is specified.

```
Hostname> enable
Hostname# show mac-address-table max-dynamic-mac-count vlan
Vlan Limit   MAC count Learning
---- ------ ---------- ------
1    160       6        YES
```

The following example displays the dynamic MAC address learning result of VLAN 1.

```
Hostname> enable
Hostname# show mac-address-table max-dynamic-mac-count vlan 1
Vlan Limit   MAC count Learning
---- ------ ---------- ------
1    160       6        YES
```

The following example displays the dynamic MAC address learning results of all interfaces for which an upper limit of learned dynamic MAC addresses is specified.

```
Hostname> enable
Hostname# show mac-address-table max-dynamic-mac-count interface
Interface             Limit   MAC count Learning
---- ------ ---------- ------
TenGigabitEthernet 0/1     160     6         YES
```

The following example displays the dynamic MAC address learning result of TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac-address-table max-dynamic-mac-count interface tenGigabitEthernet
0/1
Interface             Limit   MAC count Learning
---- ------ ---------- ------
TenGigabitEthernet 0/1    160     6         YES
```

Table 1-9 Output Fields of the show mac-address-table max-dynamic-mac-count Command

Field	Description
Vlan	VLAN ID
Interface	Interface name
Limit	Upper limit of learned MAC addresses
MAC count	Number of dynamic MAC addresses learned from the current VLAN

Field	Description
Learning	Status of the MAC address learning function for an interface or a VLAN ● **YES**: enabled ● **NO**: disabled

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show mac-address-table interface

Function

Run the **show mac-address-table interface** command to display static or dynamic MAC address entries for a specified interface.

Syntax

show mac-address-table interface *interface-type interface-number*

Parameter Description

interface *interface-type interface-number*: Displays the MAC address entries for a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

You can use this command to display all static and dynamic MAC address entries for a specified interface.

Examples

The following example displays all MAC addresses for TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac-address-table interface tenGigabitEthernet 0/1
Vlan       MAC Address         Type    Interface           Live Time
---------- ------------------- ------- ------------------- -------------
1          00d0.f800.1001      STATIC   tTenGigabitEthernet 0/1 -
1          00d0.f800.1002      STATIC   TenGigabitEthernet 0/1 -
```

```
1          00d0.f800.1003      STATIC   TenGigabitEthernet 0/1 -
1          00d0.f800.1004      STATIC   TenGigabitEthernet 0/1 -
```

Table 1-10 Output Fields of the show mac-address-table interface Command

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address entry ● **DYNAMIC**: dynamic MAC address entry
Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show mac-address-table notification

Function

Run the **show mac-address-table notification** command to display MAC address change notifications.

Syntax

show mac-address-table notification [**interface** [*interface-type interface-number*] | **history**]

Parameter Description

interface *interface-type interface-number*: Displays configurations of the MAC address change notification function for a specified interface. If no interface is specified, the configurations of the MAC address change notification function for all interfaces are displayed.

history: Displays the history table for MAC address change notifications.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If you do not specify any parameter in this command, the global configurations of the MAC address change notification function are displayed.

Examples

The following example displays the global configurations of the MAC address change notification function.

```
Hostname> enable
Hostname# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Table 1-11 Output Fields of the show mac-address-table notification Command

Field	Description
Interval(Sec)	Interval for generating MAC address change notifications
Maximum History Size	Maximum number of entries in the history table for MAC address change notifications.
Current History Size	Number of current records in the history table for MAC address change notifications.

The following example displays the configurations of the MAC address change notification function for TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac-address-table notification interface tenGigabitEthernet 0/1
Interface             MAC Added Trap    MAC Removed Trap
--------------------- ----------------- --------------------
TenGigabitEthernet 0/1   Enabled           Enabled
```

Table 1-12 Output Fields of the show mac-address-table notification interface Command

Field	Description
Interface	Interface name
MAC Added Trap	Status of the MAC address addition notification function ● **Enabled**: enabled. ● **Disabled**: disabled.
MAC Removed Trap	Status of the MAC address deletion notification function. ● **Enabled**: enabled. ● **Disabled**: disabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show mac-address-table static

Function

Run the **show mac-address-table static** command to display the static MAC address entries.

Syntax

show mac-address-table static [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]

Parameter Description

mac-address: Displays the static MAC address entry of a specified MAC address.

interface *interface-type interface-number*: Displays the MAC address entries for a specified interface.

vlan *vlan-id*: Displays the static MAC address entries for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If you do not specify any parameter in this command, all static MAC address entries are displayed.

Examples

The following example displays all static MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table static
Vlan    MAC Address     Type        Interface            Live Time
------ ---------------- ---------- ----------------------------------
1      00d0.f800.1001   STATIC     tTenGigabitEthernet 0/1   -
1      00d0.f800.1002   STATIC     TenGigabitEthernet 0/1   -
1      00d0.f800.1003   STATIC     TenGigabitEthernet 0/1   -
```

Table 1-13 Output Fields of the show mac-address-table static Command

Field	Description

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address.
Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show mac-address-table evpn

Function

Run the **show mac-address-table evpn** command to display the MAC address entries for an EVPN.

Syntax

show mac-address-table evpn

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays MAC address information for an EVPN.

```
Hostname> enable
Hostname# show mac-address-table evpn
VLAN/VSI/VNI   MAC Address     Type    Learned-From         Live Time
-------------- -------------- -------- -------------------- -------------
```

```
-/1         0026.8b06.64d6     DYNAMIC  TenGigabitEthernet 0/3   0d 16:06:23
-/1         4236.3234.3766     STATIC   TenGigabitEthernet 0/3   -
```

Table 1-14 Output Fields of the show mac-address-table evpn Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 show mac-address-table mlag

Function

Run the **show mac-address-table mlag** command to display the MAC address entries for an MLAG.

Syntax

show mac-address-table mlag

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays MAC address entries for an MLAG.

```
Hostname> enable
Hostname# show mac-address-table mlag
VLAN/VSI/VNI   MAC Address         Type     Learned-From           Live Time
-------------- -------------- -------- ----------------------- -------------
-/1/-          0026.8b06.64d6      DYNAMIC  TenGigabitEthernet 0/3   0d 16:06:23
-/1/-          4236.3234.3831      STATIC   TenGigabitEthernet 0/3    -
```

Table 1-15 Output Fields of the show mac-address-table mlag Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.24 show mac-address-table vlan

Function

Run the **show mac-address-table vlan** command to display all types of MAC address entries for a specified VLAN.

Syntax

show mac-address-table vlan [*vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

vlan *vlan-id*: Displays the MAC address entries for a specified VLAN. *vlan-id*: ID of the specified VLAN. The value range is from 1 to 4094.

interface *interface-type interface-number*: Displays the MAC address entries for a specified interface. If you do not specify this parameter, the MAC address entries for a specified VLAN on all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays all types of MAC address entries for VLAN 1.

```
Hostname> enable
Hostname# show mac-address-table vlan 1
Vlan    MAC Address     Type       Interface                Live Time
------ -------------- ---------- ------------------------ -------------
1      00d0.f800.1001  STATIC    TenGigabitEthernet 0/1       -
1      00d0.f800.1002  STATIC    TenGigabitEthernet 0/1       -
1      00d0.f800.1003  STATIC    TenGigabitEthernet 0/1       -
```

Table 1-16 Output Fields of the show mac-address-table vlan Command

Field	Description
Vlan	VLAN to which the MAC address belongs.
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address
Interface	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.25 show mac-address-table vsi

Function

Run the **show mac-address-table vsi** command to display all types of MAC address entries for a specified VSI.

Syntax

show mac-address-table vsi *vsi-id*

Parameter Description

vsi-id: ID of a VSI for which MAC address entries are to be displayed. The value range is from 1 to 2147483647.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays all types of MAC address entries for VSI 1.

```
Hostname> enable
Hostname# show mac-address-table vsi 1
VLAN/VSI/VNI   MAC Address         Type    Learned-From               Live Time
-------------- ------------------- ------- -------------------------- -------------
/1/-         1234.2222.3333        STATIC   TenGigabitEthernet 0/1          -
```

Table 1-17 Output Fields of the show mac-address-table vsi Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show mac-address-table vni

Function

Run the **show mac-address-table vni** command to display all types of MAC address entries for a specified VNI.

Syntax

show mac-address-table vni *vni-id*

Parameter Description

vni-id: ID of a specified VNI for which the MAC address entries are to be displayed. The value range is from 1 to 16777215.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays all types of MAC address entries for VNI 1.

```
Hostname> enable
Hostname# show mac-address-table vni 1
VLAN/VSI/VNI   MAC Address     Type    Learned-From            Live Time
-------------- ---------------- ------- ---------------------- -------------
-/1          0026.8b06.64d6   DYNAMIC  TenGigabitEthernet 0/3     0d 16:06:23
```

Table 1-18 Output Fields of the show mac-address-table vni Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address

Field	Description
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show mac-address-table all

Function

Run the **show mac-address-table all** command to display all types of MAC address entries.

Syntax

show mac-address-table all

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays all types of MAC address entries.

```
Hostname> enable
Hostname# show mac-address-table all
VLAN/VSI/VNI   MAC Address         Type    Learned-From          Live Time
-------------- ------------------- ------- --------------------- -------------
-/1        0026.8b06.64d6      DYNAMIC  TenGigabitEthernet 0/3     0d 16:06:23
1/-        0000.2692.0000      DYNAMIC  TenGigabitEthernet 0/15    0d 08:01:25
1/-        0012.3247.48ae      DYNAMIC  TenGigabitEthernet 0/15    0d 08:02:40
1/-        001a.a968.e78c      DYNAMIC  TenGigabitEthernet 0/15    0d 06:21:27
```

```
1/-        0023.24e3.f694      DYNAMIC  TenGigabitEthernet 0/15    0d 08:00:34
```

Table 1-19 Output Fields of the show mac-address-table all Command

Field	Description
VLAN/VSI/VNI	VLAN/VSI/VNI to which the MAC address belongs
MAC Address	MAC address
Type	Type of the MAC address: ● **STATIC**: static MAC address ● **DYNAMIC**: dynamic MAC address
Learned-From	Interface to which the MAC address belongs
Live Time	Keep-alive time of the MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 snmp trap mac-notification

Function

Run the **snmp trap mac-notification** command to enable the MAC address change notification function for an interface.

Run the **no** form of this command to disable the MAC address change notification function.

Run the **default** form of this command to disable the MAC address change notification function.

The MAC address change notification function is disabled by default.

Syntax

snmp trap mac-notification { **added** | **removed** }

no snmp trap mac-notification { **added** | **removed** }

default snmp trap mac-notification { **added** | **removed** }

Parameter Description

added: Enables the MAC address addition notification function.

removed: Enables the MAC address deletion notification function.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the MAC address change notification function is enabled on a device, the device generates a MAC address change notification message when the device learns a new MAC address or has aged a learned MAC address.

You can run the **show mac-address-table notification** command to display configurations of the MAC address change notification function.

Examples

The following example enables the Trap notification message function on TenGigabitEthernet 0/1 for sending a notification message upon MAC address addition.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# snmp trap mac-notification added
```

The following example enables the Trap notification message function on TenGigabitEthernet 0/1 for sending a notification message upon MAC address deletion.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# snmp trap mac-notification removed
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **snmp-server enable traps mac-notification** (network management and monitoring/SNMP)
- **snmp-server host** (network management and monitoring/SNMP)
- **mac-address-table notification**

1.29 mac-address-table warning-interval

Function

Run the **mac-address-table warning-interval** command to configure the interval for reporting MAC address table usage alarms.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the alarm interval to the default value.

The interval for reporting MAC address table usage alarms is 3600s (one hour) by default.

Syntax

mac-address-table warning-interval *interval*

no mac-address-table warning-interval

default mac-address-table warning-interval

Parameter Description

interval: Alarm interval. The value is **0** or ranges from 10 to 7200. The value **0** indicates that the MAC address table usage alarm function is disabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for reporting MAC address table usage alarms to 1800s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table warning-interval 1800
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 mac-address-table warning-threshold

Function

Run the **mac-address-table warning-threshold** command to configure the upper and lower limits for reporting MAC address table usage alarms.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

By default, the upper and lower limits for reporting MAC address table usage alarms are 80% and 70%, respectively.

Syntax

mac-address-table warning-threshold upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

no mac-address-table warning-threshold

default mac-address-table warning-threshold

Parameter Description

upper-limit-value: Upper limit for reporting MAC address table usage alarms. The value range is from 1 to 100.

lower-limit-value: Lower limit for reporting MAC address table usage alarms. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The value of *lower-limit-value* must be smaller than that of *upper-limit-value*.

If an alarm indicating that the usage exceeds the upper limit is reported, the MAC address table usage exceeds the normal standard. In this case, you are advised to offload the network traffic or expand the capacity.

Examples

The following example sets the upper and lower limits for reporting MAC address table usage alarms to 90% and 30%, respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table warning-threshold upper-limit 90 lower-limit 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 mac-address-table flapping-logging

Function

Run the **mac-address-table flapping-logging** command to enable MAC address flapping detection.

Run the **no** form or the **default** form of this command to disable MAC address flapping detection.

MAC address flapping detection is disabled by default.

Syntax

mac-address-table flapping-logging

no mac-address-table flapping-logging

default mac-address-table flapping-logging

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By enabling MAC address flapping detection, you can effectively monitor MAC address flapping events on the L2 network. Each time a MAC address flapping event occurs, the device reports a log alarm message.

Examples

The following example enables MAC address flapping detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table flapping-logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac-address-table flapping action**

1.32 mac-address-table flapping action

Function

Run the **mac-address-table flapping action** command to enable the MAC address flapping protection policy.

Run the **no** form of this command to disable the MAC address flapping protection policy.

Run the **default** form of this command to disable the MAC address flapping protection policy.

The MAC address flapping protection policy is disabled by default.

Syntax

mac-address-table flapping action { **error-down** | **priority** *priority-number* }

no mac-address-table flapping action { **error-down** | **priority** }

default mac-address-table flapping action { **error-down** | **priority** }

Parameter Description

error-down: Specifies the policy applied to an interface: disabling an interface when a MAC address flapping event occurs on this interface.

priority *priotiry-number*: Specifies the priority of the error-down policy on an interface. The value range is from 0 to 5, and the default value is **0**. A larger value means a higher priority.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This function takes effect only when MAC address flapping detection is enabled.

When the device detects a MAC address flapping event between two interfaces with different priorities, the device reports an alarm message and disables the low-priority interface.

If you run the **default interface** command in global configuration mode for an interface that includes L2 subinterfaces, the MAC flapping protection policy applied to the interface is restored to the default configuration.

Examples

The following example enables MAC address flapping detection and disables TenGigabitEthernet 0/1 when a MAC address flapping event occurs in this interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table flapping-logging
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# mac-address-table flapping action
error-down
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac-address-table flapping-logging**

1 MAC Loopback Commands

Command	Function
mac-loopback	Configure an interface as a loopback interface and enable MAC loopback on the interface.
show mac-loopback	Display the loopback interface configuration status of the current device.

1.1 mac-loopback

Function

Run the **mac-loopback** command to configure an interface as a loopback interface and enable MAC loopback on the interface.

Run the **no** form of this command to disable MAC loopback on the interface.

Run the **default** form of this command to restore the default configuration.

MAC loopback is disabled for an interface by default.

Syntax

mac-loopback

no mac-loopback

default mac-loopback

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can use this command to configure an interface as a MAC loopback interface.

Examples

The following example configures TenGigabitEthernet 0/1 as a loopback interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# mac-loopback
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show mac-loopback**

1.2 show mac-loopback

Function

Run the **show mac-loopback** command to display the loopback interface configuration status of the current device.

Syntax

show mac-loopback

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can use this command to display the loopback interface configuration status of the current device.

Examples

The following example displays the loopback interface configuration status of the current device.

```
Hostname> enable
Hostname# show mac-loopback
Interface             MAC
TenGigabitEthernet 0/1   Loopback
TenGigabitEthernet 0/2   Loopback
```

Table 1-1 Output Fields of the show mac-loopback Command

Field	Description
Interface	Interface
Loopback	Loopback interface

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 VLAN Commands

Command	Function
add interface	Add one access port or a group of access ports to the current virtual local area network (VLAN).
interface vlan	Create a switch virtual interface (SVI) for a VLAN and enter the SVI configuration mode.
name	Configure a name for a VLAN.
show vlan	Display member port information of a VLAN.
switchport access vlan	Add an access port to a specified VLAN.
switchport hybrid allowed vlan	Configure tagged and untagged allowed VLANs for a hybrid port.
switchport hybrid native vlan	Configure a native VLAN for a hybrid port.
switchport mode	Configure the L2 interface mode.
switchport trunk allowed vlan	Configure allowed VLANs for a trunk port or an uplink port.
switchport trunk native vlan	Configure a native VLAN for a trunk or uplink port.
vlan	Create a VLAN or enter the VLAN configuration mode.

1.1 add interface

Function

Run the **add interface** command to add one access port or a group of access ports to the current virtual local area network (VLAN).

Run the **no** form of this command to restore the current VLAN (other than VLAN 1) of one access port or a group of access ports to VLAN 1.

Run the **default** form of this command to delete one access port or a group of access ports from the current VLAN.

All L2 Ethernet interfaces belong to VLAN 1 by default, and no port exists in new VLANs.

Syntax

add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

no add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

default add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

Parameter Description

interface *interface-type interface-number*: Specifies an interface in format of *interface-type [slot /] int.* The values are L2 Ethernet interfaces or L2 aggregation ports (APs).

range *interface-type interface-range*: Specifies a group of interfaces in format of *interface-type [slot /] intmin – intmax,int*. The values are L2 Ethernet interfaces or L2 APs.

Command Modes

VLAN configuration mode

Default Level

14

Usage Guidelines

This command takes effect to access ports only. If the interface is, for example, a trunk port, run the **switchport trunk allowed vlan** { **add** *vlan-list* | **remove** *vlan-list* } command to modify the allowed VLANs list of the interface.

If the interface is not an L2 access port, run the **switchport** command to configure the interface as an L2 interface, and run the **switchport mode access** command to configure the interface as an access port.

The configuration effect of this command is equivalent to that of the **switchport access vlan** *vlan-id* command that configures a VLAN for an interface in interface configuration mode. If both commands are configured, the later one prevails.

You must run the **interface aggregateport** *ap-number* command to create an AP before adding the AP to a VLAN. When you use this command to add an L2 AP to the current VLAN, the configuration takes effect to the L2 AP only.

Examples

The following example adds an access port GigabitEthernet 0/10 to VLAN 20 and displays the status and information about GigabitEthernet 0/10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 20
Hostname(config-vlan)# add interface gigabitethernet 0/10
Hostname(config-vlan)# show interface gigabitethernet 0/10 switchport
Interface             Switchport  Mode     Access  Native  Protected VLAN lists
--------------------   ----------  ------   ------  ------  ---------  ----------
GigabitEthernet 0/10   enabled     ACCESS   20    1     Disabled  ALL
```

The following example adds a group of access ports to VLAN 20 and displays the member port information of the VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 20
Hostname(config-vlan)# add interface range gigabitethernet 0/1-10,0/12-14,0/15
Hostname# show vlan
VLAN Name        Status            Ports
---------        ------            ----------------------------
1    VLAN0001    STATIC            Gi0/11,Gi0/16,Gi0/17,Gi0/18
                                   Gi0/19,Gi0/20,Gi0/21,Gi0/22
                                   Gi0/23,Gi0/24
20   VLAN0020    STATIC              Gi0/1,Gi0/2,Gi0/3,Gi0/4
                                   Gi0/5,Gi0/6,Gi0/7,Gi0/8
                                   Gi0/9,Gi0/10,Gi0/12,Gi0/13,
                                   Gi0/14,Gi0/15
```

The following example adds AggregatePort 10 to VLAN 20 and displays the information about AggregatePort 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interfaces aggregateport 10
Hostname(config-if-AggregatePort 1)# show interface aggregateport 10 switchport
Interface          Switchport    Mode    Access   Native    Protected   VLAN lists
----------------    ----------    -----    ------   ------    --------
-----------
AggregatePort 10    enabled       ACCESS   1       1        Disabled    ALL
Hostname(config-if-AggregatePort 1)# exit
Hostname(config)# vlan 20
Hostname(config-vlan)# add interface aggregateport 10
Hostname(config-vlan)# show interface aggregateport 10 switchport
Interface          Switchport    Mode    Access   Native    Protected   VLAN lists
----------------    ----------    -----    ------   ------    --------
-----------
```

```
AggregatePort 10    enabled       ACCESS   20      1        Disabled    ALL
Hostname(config-vlan)# show vlan
VLAN Name        Status             Ports
---------        ------             ---------------------------------
1    VLAN0001    STATIC             Gi0/11,Gi0/16,Gi0/17,Gi0/18
                                    Gi0/19,Gi0/20,Gi0/21,Gi0/22
                                    Gi0/23,Gi0/24
20   VLAN0020     STATIC             Gi0/1,Gi0/2,Gi0/3,Gi0/4
                                    Gi0/5,Gi0/6,Gi0/7,Gi0/8
                                    Gi0/9,Gi0/10,Gi0/12,Gi0/13,
                                    Gi0/14,Gi0/15,Ag10
```

Notifications

N/A

Common Errors

- The interface to be added or deleted is not an L2 switch port.
- The interface to be added or deleted is not an access port. For example, the allowed VLANs of the trunk port cannot be modified using this command.
- The interface to be added or deleted is a member port of the AP, or the AP is not created in advance.
- When you add a group of ports to a VLAN, the **range** parameter is not set.

Platform Description

N/A

Related Commands

- **interface aggregateport** (interface/link AP)
- **Switchport** (interface/Ethernet interface)
- **show interfaces switchport** (interface/Ethernet interface)
- **show vlan**
- **switchport access vlan**
- **switchport mode**
- **vlan**

1.2 interface vlan

Function

Run the **interface vlan** command to create a switch virtual interface (SVI) for a VLAN and enter the SVI configuration mode.

Run the **no** form of this command to delete an SVI from the VLAN.

No SVI is configured for a VLAN by default.

Syntax

interface vlan *vlan-id*

no interface vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094. Only one VLAN can be configured.

Command Modes

Global configuration mode

VLAN configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enters the SVI interface configuration mode of VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vlan**

1.3 name

Function

Run the **name** command to configure a name for a VLAN.

Run the **no** form of this command to restore the VLAN name to the default value.

Run the **default** form of this command to restore the VLAN name to the default value.

The default name of a VLAN is "VLAN+VLAN ID". For example, the default name of VLAN 2 is VLAN0002.

Syntax

name *vlan-name*

no name

default name

Parameter Description

vlan-name: New name of a VLAN, used to replace the default VLAN name "VLAN+VLAN ID".

Command Modes

VLAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the name of VLAN 20 as **office 10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 20
Hostname(config-vlan)# name office 10
Hostname(config-vlan)# show vlan
VLAN Name        Status            Ports
---------        ------           ------------------------------
1    VLAN0001    STATIC            Gi0/11,Gi0/16,Gi0/17,Gi0/18
                                  Gi0/19,Gi0/20,Gi0/21,Gi0/22
                                  Gi0/23,Gi0/24
20   office 10    STATIC           Gi0/1,Gi0/2,Gi0/3,Gi0/4
                                  Gi0/5,Gi0/6,Gi0/7,Gi0/8
                                  Gi0/9,Gi0/10,Gi0/12,Gi0/13,
                                  Gi0/14,Gi0/15,Ag10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vlan**
- **vlan**

1.4 show vlan

Function

Run the **show vlan** command to display member port information of a VLAN.

Syntax

show vlan [**id** *vlan-id*]

Parameter Description

id *vlan-id*: Specifies a VLAN ID. The value range is from 1 to 4094. If this parameter is configured, only member port information of a single VLAN is displayed. If this parameter is not configured, member port information of all VLANs is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays member port information of VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config-vlan)# show vlan id 20
VLAN Name                           Status    Ports
---- -------------------------------  -------  -------
20   VLAN0020                       STATIC    Gi0/1
```

The following example displays configurations and member port information of All VLANs.

```
Hostname(config-vlan)# show vlan
VLAN Name                           Status    Ports
---- -------------------------------  ------    ---------------------------------
1   VLAN0001                       STATIC    Gi0/1, Gi0/2, Gi0/4, Gi0/5
                                             Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                             Gi0/10, Gi0/11, Gi0/12, Gi0/13
                                             Gi0/14, Gi0/15, Gi0/16, Gi0/17
                                             Gi0/18, Gi0/19, Gi0/20, Gi0/21
                                             Gi0/22, Gi0/23, Gi0/24
2-3 VLAN0002-VLAN0003              STATIC    Gi0/1
20  VLAN0020                      STATIC    Gi0/1
```

Table 1-1 Output Fields of the show vlan Command

Field	Description
VLAN	VLAN ID
Name	VLAN name
Status	Attribute of a VLAN ● **STATIC**: static VLAN ● **Dynamic**: dynamic VLAN ● **PRIVATE**: primary or secondary VLAN of a private VLAN ● **SUPER**: super VLAN ● **SUB**: sub VLAN of a super VLAN
Ports	Ports that are added to this VLAN

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 switchport access vlan

Function

Run the **switchport access vlan** command to add an access port to a specified VLAN.

Run the **no** form of this command to restore the current VLAN of the access port to VLAN 1.

Run the **default** form of this command to restore the current VLAN of the access port to the default VLAN.

The access port belongs to VLAN 1 by default.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

default switchport access vlan

Parameter Description

vlan *vlan-id*: Specifies the ID of a VLAN to which an access port is to be added. The value range is from 1 to 4094. Only one VLAN can be configured.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the specified VLAN already exists, the port is added to the VLAN. If the specified VLAN does not exist, the system automatically creates this VLAN and adds the interface to the VLAN.

If the interface to be added is a trunk port, the port cannot be added to the specified VLAN.

Examples

The following example adds the access port GigabitEthernet 0/1 to VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport mode**

1.6 switchport hybrid allowed vlan

Function

Run the **switchport hybrid allowed vlan** command to configure tagged and untagged allowed VLANs for a hybrid port.

Run the **no** form of this command to restore the allowed VLANs of a hybrid port to default values.

Run the **default** form of this command to restore the allowed VLANs of a hybrid port to default values.

By default, the allowed VLANs of the hybrid port are tagged VLANs 2 to 4094 and untagged VLAN 1.

Syntax

switchport hybrid allowed vlan { [**add**] **tagged** | [**add**] **untagged** | **only tagged** | **remove** } *vlan-list*

no switchport hybrid allowed vlan

default switchport hybrid allowed vlan

Parameter Description

vlan-list: VLAN list. The value range is from 1 to 4094. The list can contain one or more VLANs. VLAN IDs are separated by commas (,). Continuous VLAN IDs are represented by connecting the first and the last VLAN IDs with a hyphen (-).

[**add**] **tagged** *vlan-list*: Adds the VLANs in *vlan-list* to the tagged allowed VLAN list of the hybrid port. Packets of the specified VLANs sent by the port are tagged. The native VLAN cannot be added to the tagged allowed VLAN list. The **add** parameter is optional. The command function is not affected by this parameter.

[**add**] **untagged** *vlan-list*: Adds the VLANs in *vlan-list* to the untagged allowed VLAN list of the hybrid port. Packets of the specified VLANs sent by the port are untagged. The native VLAN must be added to the untagged allowed VLAN list. The **add** parameter is optional. The command function is not affected by this parameter.

only tagged *vlan-list*: Adds the VLANs in *vlan-list* to the tagged allowed VLAN list of the hybrid port and removes other tagged VLANs from the allowed VLAN list. Other untagged VLANs are not affected.

remove *vlan-list*: Removes the VLANs in *vlan-list* from the allowed VLAN list of the hybrid port. The native VLAN can be removed as well.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the L2 interface GigabitEthernet 0/1 as a hybrid port and removes the default allowed VLANs 1 to 4094.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/1)# show interface gigabitethernet 0/1
switchport
Interface           Switchport   Mode    Access   Native   Protected   VLAN lists
------------------   ----------   ------   ------   ------   ---------   -------
GigabitEthernet 0/1   enabled     HYBRID   1       1       Disabled    ALL
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan remove 1-4094
Hostname(config-if-GigabitEthernet 0/1)# show interface gigabitethernet 0/1
switchport
Interface          Switchport        Mode     Access   Native    Protected   VLAN
lists
------------------   ----------   ------   ------   ------   ---------   -------
GigabitEthernet 0/1   enabled   HYBRID     1        1       Disabled
```

The following example adds VLAN 20 and VLAN 30 to the allowed VLAN list of the hybrid port and forwards packets of VLAN 20 and VLAN 30 in untagged mode.

```
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan add untagged
30
```

The following example adds VLAN 40 and VLAN 50 to the allowed VLAN list of the hybrid port and forwards packets of VLAN 40 and VLAN 50 in tagged mode.

```
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan tagged 40
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan tagged 50
```

The following example configures the native VLAN of the hybrid port GigabitEthernet 0/1 as VLAN 2.

```
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 2
Hostname(config-if-GigabitEthernet 0/1)# show interface gigabitethernet 0/1
switchport
Interface     Switchport        Mode     Access   Native    Protected   VLAN lists
---------     ----------     ---------   ------     ------   ---------  -----------
GigabitEthernet 0/1   enabled   HYBRID     1         2       Disabled   20,30,40,50
```

The following example retains VLAN 20 as the allowed VLAN for the hybrid port, deletes other VLANs (VLAN 30, VLAN 40, and VLAN 50), and forwards packets of VLAN 20 in tagged mode.

```
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan only tagged
20
```

The following example deletes the allowed VLAN 20 from the hybrid port.

```
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan remove 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show interface** (interface/Ethernet interface)
- **switchport mode**

1.7 switchport hybrid native vlan

Function

Run the **switchport hybrid native vlan** command to configure a native VLAN for a hybrid port.

Run the **no** form of this command to restore the native VLAN to VLAN 1.

Run the **default** form of this command to restore the native VLAN to VLAN 1.

The native VLAN of the hybrid port is VLAN 1 by default.

Syntax

switchport hybrid native vlan *vlan-id*

no switchport hybrid native vlan

default switchport hybrid native vlan

Parameter Description

vlan-id: Native VLAN of the hybrid port. The value range is from 1 to 4094. Only one VLAN can be configured.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Packets of the native VLAN sent by the hybrid port are untagged. Packets of an allowed VLAN (other than the native VLAN) sent by the hybrid port can be tagged or untagged.

When the hybrid port receives an untagged packet, the hybrid port considers that the packet comes from the native VLAN of this port.

Examples

The following example configures the native VLAN of the hybrid port GigabitEthernet 0/1 as VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 2
Hostname(config-if-GigabitEthernet 0/2)# show interface gigabitethernet 0/2
switchport
Interface          Switchport Mode     Access Native Protected VLAN lists
-------------------- ---------- --------- ------ ------ --------- ----------
GigabitEthernet 0/1  enabled    HYBRID    1      2     Disabled  ALL
```

Notifications

N/A

Common Errors

No native VLAN is created before it is configured. In this case, VLAN configuration is not completed though the returned value is correct.

Platform Description

N/A

Related Commands

- **switchport mode**

1.8 switchport mode

Function

Run the **switchport mode** command to configure the L2 interface mode.

Run the **no** form of this command to restore the L2 interface mode to the default value.

Run the **default** form of this command to restore the L2 interface mode to the default value.

The L2 interface mode is **access** by default.

Syntax

switchport mode { **access** | **trunk** | **hybrid** | **uplink** }

no switchport mode

default switchport mode

Parameter Description

access: Configures the L2 interface mode as **access**.

trunk: Configures the L2 interface mode as **trunk**.

hybrid: Configures the L2 interface mode as **hybrid**.

Uplink: Configures the L2 interface mode as **uplink**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- Before you configure the L2 interface mode as **access**, **trunk**, **hybrid**, or **uplink**, ensure that the interface is an L2 interface. You can run the **switchport** command to configure an interface as an L2 interface, and run the **no switchport** command to configure an interface as an L3 interface. When you configure an interface as an L2/L3 interface, all attributes of the interface are restored to the default values in this interface mode.
- If the L2 interface mode is **access**, this interface can be assigned to one VLAN only. Therefore, the native VLAN is the allowed VLAN, and this VLAN is VLAN 1 by default. You can run the **switchport access vlan** command to assign this interface to a specified VLAN. Packets sent by the access port are untagged.
- If the L2 interface mode is **trunk**, this interface has one native VLAN, and this VLAN is VLAN 1 by default. You can run the **switchport trunk native vlan** command to configure the native VLAN for the interface. The allowed VLANs are VLANs 1 to 4094 by default, namely, all VLANs. You can run the **switchport trunk allowed vlan** command to configure allowed VLANs for the interface. The native VLAN can be excluded from the allowed VLANs. In this case, data of the native VLAN cannot be forwarded by the port. Packets of the native VLAN forwarded by the trunk port are untagged, and packets of other allowed VLANs are tagged.
- If the L2 interface mode is **uplink**, this interface has one native VLAN, and this VLAN is VLAN 1 by default. You can run the **switchport trunk native vlan** command to configure a native VLAN for the interface. The allowed VLANs are VLANs 1 to 4094 by default, namely, all VLANs. You can run the **switchport trunk allowed vlan** command to configure allowed VLANs for the interface. Unlike the trunk port, the uplink port

forwards tagged packets.

- If the L2 interface mode is **hybrid**, this interface has one native VLAN, and this VLAN is VLAN 1 by default. You can run the **switchport hybrid native vlan** command to configure a native VLAN for the interface. The allowed VLANs are VLANs 1 to 4094 by default, namely, all VLANs. You can run the **switchport hybrid allowed vlan** command to configure allowed VLANs for the interface. Packets of the native VLAN sent by the hybrid port are untagged. Unlike the trunk port, the hybrid port can forward tagged and untagged packets of allowed VLANs other than the native VLAN.
- You can run the **show interface** [*interface id*] **switch** command to display interface configurations.

Examples

The following example configures GigabitEthernet 0/1 as an L2 interface and then configures the interface as an access port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport
Hostname(config-if-GigabitEthernet 0/1)# switchport mode access
```

The following example configures the L2 interface GigabitEthernet 0/1 as a trunk port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

The following example configures the L2 interface GigabitEthernet 0/1 as an uplink port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode uplink
```

The following example configures the L2 interface GigabitEthernet 0/1 as a hybrid port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport access vlan**

1.9 switchport trunk allowed vlan

Function

Run the **switchport trunk allowed vlan** command to configure allowed VLANs for a trunk port or an uplink port.

Run the **no** form of this command to restore the allowed VLANs of the trunk or uplink port to default values.

Run the **default** form of this command to restore the allowed VLANs of the trunk or uplink port to default values.

The allowed VLANs of the trunk port are VLANs 1 to 4094 and the allowed VLANs of the uplink port are VLANs 1 to 4094 by default.

Syntax

switchport trunk allowed vlan { **all** | { **add** | **remove** | **except** | **only** } *vlan-list* }

no switchport trunk allowed vlan

default switchport trunk allowed vlan

Parameter Description

all: Adds all VLANs to the allowed VLAN list of the trunk port.

vlan-list: VLAN list. The value range is from 1 to 4094. The list can contain one or more VLANs. VLAN IDs are separated by commas (,). Continuous VLAN IDs are represented by connecting the first and the last VLAN IDs with a hyphen (-).

add *vlan-list*: Adds the VLANs in *vlan-list* to the allowed VLAN list of the trunk port.

remove *vlan-list*: Removes the VLANs in *vlan-list* from the allowed VLAN list of the trunk port.

except *vlan-list*: Adds all the VLANs other than those in *vlan-list* to the allowed VLAN list of the trunk port.

only *vlan-list*: Adds the VLANs in *vlan-list* to the allowed VLAN list of the trunk port and removes other VLANs from the allowed VLAN list.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can configure an allowed VLAN list for the trunk or uplink port to direct traffic of the specified VLANs to pass through this trunk or uplink port.

You can run the **show interfaces** command to display interface configurations.

Examples

The following example removes VLAN 2 from the allowed VLAN list of the trunk port GigabitEthernet 0/10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 2
```

The following example adds VLANs other than VLAN 10 to the allowed VLAN list of the trunk port GigabitEthernet 0/10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10
```

The following example adds only VLAN 10 to the allowed VLAN list of the trunk port GigabitEthernet 0/10 and removes other VLANs from the allowed list of the port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan only 10
```

The following example removes VLAN 10 from the allowed VLAN list of the uplink port GigabitEthernet 0/10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode uplink
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 10
```

The following example adds VLANs other than VLAN 10 to the allowed VLAN list of the uplink port GigabitEthernet 0/10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode uplink
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10
```

The following example adds only VLAN 10 to the allowed VLAN list of the uplink port GigabitEthernet 0/10 and removes other VLANs from the allowed list of the port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode uplink
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan only 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show interface** (interface/Ethernet interface)
- **switchport mode**

1.10 switchport trunk native vlan

Function

Run the **switchport trunk native vlan** command to configure a native VLAN for a trunk or uplink port.

Run the **no** form of this command to restore the native VLAN of a port to VLAN 1.

Run the **default** form of this command to restore the native VLAN of a port to VLAN 1.

The native VLAN of a trunk or uplink port is VLAN 1 by default.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

default switchport trunk native vlan

Parameter Description

vlan-id: ID of the configured native VLAN. The value range is from 1 to 4094. Only one VLAN can be configured.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After you configure a native VLAN for the trunk port, when the trunk port receives an untagged packet, the trunk port considers that the packet comes from the native VLAN of this port.

Packets of the native VLAN sent by the port are untagged.

Examples

The following example configures the native VLAN of the trunk port GigabitEthernet 0/10 as VLAN 10.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

The following example configures the native VLAN of the uplink port GigabitEthernet 0/10 as VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport mode uplink
Hostname(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport mode**

1.11 vlan

Function

Run the **vlan** command to create a VLAN or enter the VLAN configuration mode.

Run the **no** form of this command to delete an existing VLAN.

Run the **default** form of this command to restore a configured VLAN to a common static VLAN.

Only one common static VLAN (VLAN 1) exists by default.

Syntax

vlan { *vlan-id* | **range** *vlan-range* }

no vlan { *vlan-id* | **range** *vlan-range* }

default vlan { *vlan-id* | **range** *vlan-range* }

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094. Only one VLAN can be configured. The default VLAN (VLAN 1) cannot be deleted.

vlan-range: Range of VLAN IDs. The value range is from 1 to 4094. The *vlan-range* field can be set to a single VLAN or a VLAN range. VLAN IDs are separated by commas (,). Continuous VLAN IDs can be represented by connecting the first and the last VLAN IDs with a hyphen (-).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates a VLAN 10 and enters the VLAN 10: configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 10
Hostname(config-vlan)#
```

The following example creates a group of VLANs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2
Hostname(config-vlan-range)# exit
Hostname(config)# vlan range 20,3,5,7-9,15-11
Hostname(config-vlan-range)# exit
```

Notifications

When an SVI has been created for a VLAN, the following notification will be displayed:

```
Vlan 10 is not allowed to be deleted.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **add**
- **interface vlan**
- **name**

1 Private VLAN Commands

Command	Function
debug bridge pvlan	Enable the private VLAN (PVLAN) debugging function.
private-vlan	Configure a common static VLAN as a PVLAN and configure the PVLAN as a primary or secondary VLAN.
show vlan private-vlan	Display the PVLAN configurations.
switchport mode private-vlan	Configure a port as a host or promiscuous port of a PVLAN.

1.1 debug bridge pvlan

Function

Run the **debug bridge pvlan** command to enable the private VLAN (PVLAN) debugging function.

Run the **no** form of this command to disable this feature.

The PVLAN debugging function is disabled by default.

Syntax

debug bridge pvlan

no debug bridge pvlan

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

Debugging information includes all errors occurring during the configuration of a PVLAN, prompt messages, and causes of VLAN and port configuration failures.

After you enable this function, you can view the configuration of the PVLAN function, packet processing by virtual interfaces, and debugging information in the case of a packet processing failure debug information, which helps you locate and diagnose faults.

Examples

The following example enables the PVLAN debug function.

```
Hostname> enable
Hostname# debug bridge pvlan
```

The following example disables the PVLAN debug function.

```
Hostname> enable
Hostname# no debug bridge pvlan
```

Debugging Information

PVLAN configuration debugging information

Debugging information: The VLAN pair (4-6) is invalid.

Explanation: When you try to associate a port with a PVLAN pair or remove the association, the PVLAN pair does not have a valid L2 association.

Cause: The specified PVLAN pair does not have a valid L2 association.

Handling suggestion: Ensure that the specified PVLAN pair has a valid L2 association.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 private-vlan

Function

Run the **private-vlan** command to configure a common static VLAN as a PVLAN and configure the PVLAN as a primary or secondary VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A VLAN is a common VLAN and has no PVLAN attribute by default.

Syntax

private-vlan { **community** | **isolated** | **primary** }

no private-vlan { **community** | **isolated** | **primary** }

default private-vlan { **community** | **isolated** | **primary** }

Parameter Description

community: Configures the VLAN as a community VLAN of the secondary VLAN.

isolated: Configures the VLAN as an isolated VLAN of the secondary VLAN.

primary: Configures the VLAN as a primary VLAN.

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

If VLAN 1 contains non-host and non-promiscuous ports, when you configure VLAN 1 as a PVLAN, an error is displayed. It is not recommended to configure VLAN 1 as a PVLAN.

You can use the **show vlan private-vlan** { **community** | **isolated** | **primary** } command to display configurations of different types of VLANs in a PVLAN.

Examples

The following example configures VLAN 90 as a primary VLAN, VLAN 91 as an isolated VLAN, and VLAN 92 as a community VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 90
Hostname(config-vlan)# private-vlan primary
Hostname(config-vlan)# exit
Hostname(config)# vlan 91
Hostname(config-vlan)# private-vlan isolated
Hostname(config-vlan)# exit
Hostname(config)# vlan 92
Hostname(config-vlan)# private-vlan community
Hostname(config-vlan)# exit
```

The following example cancels the attributes of the primary VLAN and secondary VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 90
Hostname(config-vlan)# no private-vlan primary
Hostname(config-vlan)# exit
Hostname(config)# vlan 91
Hostname(config-vlan)# no private-vlan isolated
Hostname(config)# vlan 92
Hostname(config-vlan)# no private-vlan community
```

The following example restores the default configurations of a VLAN, that is, restores the PVLAN to a common VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 90
Hostname(config-vlan)# default private-vlan primary
Hostname(config-vlan)# exit
Hostname(config)# vlan 91
Hostname(config-vlan)# default private-vlan isolated
Hostname(config-vlan)# exit
Hostname(config)# vlan 92
Hostname(config-vlan)# default private-vlan community
```

Notifications

When you try to use the **no private-vlan** command to restore a PVLAN to a common static VLAN and the { **community** | **isolated** | **primary** } parameter in the command is inconsistent with the PVLAN mode of the PVLAN, the following notification will be displayed:

```
Types of private VLANs do not match
```

When you try to configure a VLAN that contains a non-host or non-promiscuous port as a PVLAN, the following notification will be displayed:

```
Setting failure for some ports are not allowed to private vlan
```

When you try to configure a VLAN that has been configured as a MAC VLAN as a PVLAN, the following notification will be displayed:

```
Can't set VLAN as non static vlan when mac vlan enabled.
```

When you try to configure a VLAN that is bound to an L3 SVI as a community VLAN, the following notification will be displayed:

```
The VLAN with svi can not be set to secondary VLAN
```

Common Errors

A dynamic VLAN is configured as a PVLAN.

Platform Description

N/A

Related Commands

- **show vlan private-vlan**

1.3 show vlan private-vlan

Function

Run the **show vlan private-vlan** command to display the PVLAN configurations.

Syntax

show vlan private-vlan { **community** | **primary** | **isolated** }

Parameter Description

primary: Displays the primary VLAN information.

community: Displays the community VLAN information.

isolated: Displays the isolated VLAN information.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example configures a PVLAN and displays PVLAN configuration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#vlan range 3-5
Hostname(config-vlan-range)# exit
Hostname(config)# vlan 3
Hostname(config-vlan)# private-vlan isolated
Hostname(config-vlan)# exit
```

```
Hostname(config)# vlan range 4-5
Hostname(config-vlan-range)# private-vlan community
Hostname(config-vlan-range)# exit
Hostname(config)# vlan 6
Hostname(config-vlan)# private-vlan primary
Hostname(config-vlan)# private-vlan association add 3-5
Hostname(config-vlan)# show vlan private

VLAN  Type      Status   Routed   Ports                  Associated VLANs
----- ---------- -------- -------- ------------------------------ ------
3     isolated   active   Disabled                          6
4     community  active   Disabled                          6
5     community  active   Disabled                          6
6     primary    active   Disabled                         3-5

Hostname(config-vlan)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/1)# switchport mode private-vlan promiscuous
Hostname(config-if-GigabitEthernet 0/1)# switchport private-vlan mapping 6 add 3-5
Hostname(config-if-GigabitEthernet 0/1)# exit

Hostname(config)# interface range gigabitethernet 0/2-4
Hostname(config-if-range)# switchport mode private-vlan host
Hostname(config-if-range)# switchport private-vlan host-association 6 3
Hostname(config-if-range)# exit

Hostname(config)# interface range gigabitethernet 0/5-8
Hostname(config-if-range)# switchport mode private-vlan host
Hostname(config-if-range)# switchport private-vlan host-association 6 4
Hostname(config-if-range)# exit

Hostname(config)# interface range gigabitethernet 0/9-12
Hostname(config-if-range)# switchport mode private-vlan host
Hostname(config-if-range)# switchport private-vlan host-association 6 5
Hostname(config-if-range)# exit
Hostname(config)# show vlan private

VLAN  Type      Status   Routed    Ports                        Associated VLANs
----- ---------- -------- -------- ------------------------------ ------------
3     isolated   active   Disabled    Gi0/2, Gi0/3, Gi0/4              6
4     community  active   Disabled    Gi0/5, Gi0/6, Gi0/7,Gi0/8        6
5     community  active   Disabled    Gi0/9, Gi0/10, Gi0/11,Gi0/12     6
6     primary    active   Disabled    Gi0/1                            3-5

Hostname(config)# interface vlan 6
```

```
Hostname(config-if-VLAN 6)# ip address 192.168.11.1 255.255.255.0
Hostname(config-if-VLAN 6)# private-vlan mapping 3-5
Hostname(config-if-VLAN 6)# exit
Hostname(config)# show vlan private

VLAN  Type      Status   Routed    Ports                          Associated VLANs
----- ---------- -------- -------- ------------------------------ -----------
3     isolated   active   Enabled   Gi0/2, Gi0/3, Gi0/4                6
4     community  active   Enabled   Gi0/5, Gi0/6, Gi0/7,Gi0/8          6
5     community  active   Enabled   Gi0/9, Gi0/10, Gi0/11,Gi0/12       6
6     primary    active   Enabled   Gi0/1                              3-5
```

Table 1-1 Output Fields of the show vlan private-vlan Command

Field	Description
VLAN	VLAN ID
Type	VLAN attribute ● **primary**: Primary VLAN ● **isolated**: Isolated VLAN ● **community**: Community VLAN
Status	L2 association status of a PVLAN ● **inactive**: No L2 association is configured for a PVLAN. ● **active**: An L2 association has been configured for a PVLAN.
Routed	L3 interface status of the primary VLAN or L3 association status of a secondary VLAN ● Disabled: No L3 interface is created for the primary VLAN or no L3 association is configured between the primary VLAN and a secondary VLAN. ● Enabled: An L3 interface has been created for the primary VLAN or an L3 association has been configured between the primary VLAN and a secondary VLAN.
Ports	Ports that are added to a PVLAN
Associated VLANs	Secondary VLANs that are L2 associated with the primary VLAN or a primary VLAN that is L2 associated with secondary VLANs

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.4 switchport mode private-vlan

Function

Run the **switchport mode private-vlan** command to configure a port as a host or promiscuous port of a PVLAN.

Run the **no switchport mode** command to restore the port to an access port.

Run the **default switchport mode** command to restore the port to an access port.

A port is an access port by default.

Syntax

switchport mode private-vlan { **host** | **promiscuous** }

no switchport mode

default switchport mode

Parameter Description

host: Configures a port as a host port of a PVLAN. A port connected to a host is configured as a host port.

promiscuous: Configures a port as a promiscuous port of a PVLAN. A port connected to a gateway or server is configured as a promiscuous port.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a port is configured as a host port and associated with a PVLAN pair by using the **switchport private-vlan host-association** *pvid svid* command, the host port can be added to a secondary VLAN. A host port in an isolated VLAN is called an isolated port, and a host port in a community VLAN is called a community port.

If a port is configured as a promiscuous port and associated with a PVLAN pair by using the **switchport private-vlan mapping** *pvid { svlist* **| add** *svlist* | **remove** *svlist* } command, the port can be added to the primary VLAN. In this case, the port is a promiscuous port.

Examples

The following example configures GigabitEthernet 0/1 as a host port of a PVLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode private-vlan host
```

The following example configures GigabitEthernet 0/2 as a promiscuous port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# sw mode private-vlan promiscuous
```

The following example restores GigabitEthernet 0/1 from a host port to an access port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no switchport mode
```

Notifications

When the MAC VLAN function is enabled on GigabitEthernet 0/1 and you try to configure the interface as a host or promiscuous port, the following notification will be displayed:

```
Can't change port mode since mac vlan has been enabled.
Operation is not supported on interface GigabitEthernet 0/1: it is not supported by
the hardware!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Super VLAN Commands

Command	Function
bcast vlan	Configure a broadcast virtual local area network (VLAN) for a super VLAN.
proxy-arp	Enable the proxy Address Resolution Protocol (ARP) function for a VLAN.
show supervlan	Display configurations of a super VLAN and its sub VLANs.
subvlan	Configure an existing common VLAN as a sub VLAN of a super VLAN.
subvlan-address-range	Configure an IP address range for a sub VLAN.
supervlan	Configure a super VLAN.

1.1 bcast vlan

Function

Run the **bcast vlan** command to configure a broadcast virtual local area network (VLAN) for a super VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No broadcast VLAN is configured in a super VLAN by default.

Syntax

bcast vlan *sub-vlan-id*

no bcast vlan

default bcast vlan

Parameter Description

bcast vlan *sub-vlan-id*: Specifies the ID of a sub VLAN that is configured as a broadcast VLAN. The value range is from 1 to 4094. The VLAN to be configured as a broadcast VLAN must be a sub VLAN of the super VLAN. Only one broadcast VLAN can be configured for a super VLAN.

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

A broadcast VLAN is configured in super VLAN configuration mode. If no broadcast VLAN is configured for a super VLAN, broadcast packets of the super VLAN are sent to all sub VLANs of the super VLAN. If a broadcast VLAN is configured, broadcast packets of the super VLAN are sent to only this broadcast VLAN.

Examples

The following example configures VLAN 2 as a super VLAN, VLANs 10, 20 and 30 as sub VLANs, and VLAN 10 as the broadcast VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 10,20,30
Hostname(config-vlan-range)# exit
Hostname(config)# vlan 2
Hostname(config-vlan)# supervlan
Hostname(config-vlan)# subvlan 10,20,30
Hostname(config-vlan)# bcast vlan 10
```

The following example removes the broadcast VLAN from VLAN 2.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# vlan 2
Hostname(config-vlan)# no bcast vlan
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show supervlan**
- **supervlan**

1.2 proxy-arp

Function

Run the **proxy-arp** command to enable the proxy Address Resolution Protocol (ARP) function for a VLAN.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The proxy ARP function of a VLAN is enabled by default.

Syntax

proxy-arp

no proxy-arp

default proxy-arp

Parameter Description

N/A

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

The proxy ARP function must be enabled for a super VLAN and its sub VLANs.

Examples

The following example enables the proxy ARP function.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# vlan 2
Hostname(config-vlan)# proxy-arp
```

The following example disables the proxy ARP function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# no proxy-arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show supervlan**

1.3 show supervlan

Function

Run the **show supervlan** command to display configurations of a super VLAN and its sub VLANs.

Syntax

show supervlan [**id** *super-vlan-id*]

Parameter Description

id *super-vlan-id*: Displays configuration of a specified super VLAN. The value range is from 1 to 4094. The specified VLAN ID must be the ID of the super VLAN. Only one VLAN ID can be specified. If the **id** *super-vlan-id* parameter is not specified, the configurations of all super VLANs and sub VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can use this command to view mappings between a super VLAN and its sub VLANs and other information.

Examples

The following example displays configurations of super VLAN 2.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# show supervlan id 2
supervlan id  supervlan arp-proxy  bcast vlan  subvlan id  subvlan arp-proxy  subvlan
ip range
------------  -------------------  ----------  ----------  -----------------
----------------
2           ON                10         10        ON   192.168.196.10 -
192.168.196.50
                                       20        ON   192.168.196.60 -
192.168.196.100
                                       30        ON   192.168.196.110 -
192.168.196.150
```

The following example displays configurations of all super VLANs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# show supervlan
supervlan id  supervlan arp-proxy  bcast vlan  subvlan id  subvlan arp-proxy  subvlan
ip range
------------  -------------------  ----------  ----------  -----------------
----------------
2           ON                10         10        ON   192.168.196.10 -
192.168.196.50
                                       20        ON   192.168.196.60 -
192.168.196.100
                                       30        ON   192.168.196.110 -
192.168.196.150
6           ON                          7-8       ON
```

Table 1-1 Output Fields of the show supervlan Command

Field	Description
supervlan id	VLAN ID of a super VLAN
supervlan arp-proxy	Whether the proxy ARP function of the super VLAN is enabled ● **ON**: Enabled ● **OFF**: Disabled
bcast vlan	Broadcast VLAN of the super VLAN
subvlan id	VLAN ID of a sub VLAN
subvlan arp-proxy	Whether the proxy ARP function of the sub VLAN is enabled ● **ON**: Enabled ● **OFF**: Disabled
subvlan ip range	IP address range of the sub VLAN

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.4 subvlan

Function

Run the **subvlan** command to configure an existing common VLAN as a sub VLAN of a super VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No common VLAN is configured as a sub VLAN of a super VLAN by default.

Syntax

subvlan [*vlan-id-list*]

no subvlan [*vlan-id-list*]

default subvlan [*vlan-id-list*]

Parameter Description

vlan-id-list: VLAN IDs that are configured as sub VLANs. The value range is from 2 to 4094. The specified VLAN must exist. VLAN 1 cannot be configured as a sub VLAN. The VLAN list contains one or more VLANs. When multiple VLANs are contained, separate VLAN IDs by a comma (,) or connect the first and last VLAN IDs with a hyphen (-) to represent continuous VLAN IDs.

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

You must enter the super VLAN configuration mode to add sub VLANs. If multiple common VLANs need to use the same network segment, configure them as sub VLANs of a super VLAN.

Examples

The following example configures VLAN 2 as a super VLAN and adds sub VLANs 10, 20 and 30 to the super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
```

```
Hostname(config-vlan)# supervlan
Hostname(config-vlan)# subvlan 10,20,30
```

The following example removes sub VLAN 20 from super VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# no subvlan 20
```

The following example removes sub VLAN 30 from super VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# default subvlan 30
```

The following example removes all sub VLANs from super VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# default subvlan
```

Notifications

When you configure sub VLANs not in super VLAN configuration mode, the following notification will be displayed:

```
vlan 2 is not a supervlan
```

If the VLAN to be configured is a dynamic VLAN rather than a static VLAN, the following notification will be displayed

```
The vlan is dynamic vlan
```

If an SVI has been configured for a super VLAN, the system assigns an L3 interface invisible to users to each sub VLAN of the super VLAN. When you add a sub VLAN to the super VLAN, the configuration may fail due to system resource deficiency. The following notification will be displayed:

```
the vlan can't be set as subvlan for lack of resources.
```

If an SVI has been configured for a VLAN, when you try to configure this VLAN as a sub VLAN of a super VLAN, the following notification will be displayed:

```
Following reason prevent some vlan to be set as supervlan 2's subvlan
The vlan has created interface
```

Common Errors

(1) An inexistent VLAN is configured as a sub VLAN.

(2) Sub VLANs are not configured in super VLAN configuration mode.

(3) A sub VLAN is added to more than one super VLAN.

(4) An L3 interface has been configured for a VLAN and then the VLAN is configured as a sub VLAN. The operation will fail.

(5) A dynamic VLAN is configured as a sub VLAN.

Platform Description

N/A

Related Commands

- **show supervlan**
- **supervlan**

1.5 subvlan-address-range

Function

Run the **subvlan-address-range** command to configure an IP address range for a sub VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IP address range is specified for a sub VLAN by default.

Syntax

subvlan-address-range *start-ip-address end-ip-address*

no subvlan-address-range

default subvlan-address-range

Parameter Description

start-ip-address: Start IP address. The value range must be in the same network segment as the gateway of the super VLAN.

end-ip-address: End IP address. The value range must be in the same network segment as the gateway of the super VLAN.

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

After an IP address range is configured for a sub VLAN, users in the sub VLAN cannot communicate when their IP addresses are out of this range.

Examples

The following example configures an IP address range for a sub VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# subvlan-address-range 192.168.23.1 192.168.23.5
```

Notifications

N/A

Common Errors

(1) A dynamic VLAN is configured as a super VLAN.

(2) The configured IP address range is not in the same network segment as the gateway of the super VLAN.

Platform Description

N/A

Related Commands

- **show supervlan**

1.6 supervlan

Function

Run the **supervlan** command to configure a super VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No common VLAN is configured as a super VLAN by default.

Syntax

supervlan

no supervlan

default supervlan

Parameter Description

N/A

Command Modes

VLAN mode

Default Level

14

Usage Guidelines

Only existent VLANs can be configured as super VLANs. VLAN 1 cannot be configured as a super VLAN.

A super VLAN cannot be configured as a sub VLAN of another super VLAN. A sub VLAN of a super VLAN cannot be configured as a super VLAN.

No physical port can be added to a super VLAN.

After a super VLAN is configured, you must configure an SVI and an IP address for this SVI so that users in sub VLANs of the super VLAN can communicate. No SVI can be configured for a sub VLAN.

Examples

The following example configures VLAN 2 as a super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# supervlan
```

Notifications

If you configure a sub VLAN of a super VLAN as a new super VLAN, the following notification will be displayed:

```
the vlan is other supervlan's subvlan
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bcast vlan**
- **show supervlan**
- **subvlan**

1 Voice VLAN Commands

Command	Function
show voice vlan	Display the configuration and current status of a voice VLAN, including the port on which the voice VLAN function is enabled and the work mode of the voice VLAN.
show voice vlan oui	Display source MAC address entries used by voice VLAN to identify voice packets on the current device.
voice vlan	Configure an existent common VLAN as a voice VLAN.
voice vlan aging	Configure aging time for a port in a voice VLAN in global configuration mode. The aging time indicates the time that the port resides in the voice VLAN when the port fails to receive voice traffic.
voice vlan cos	Configure the CoS value for voice traffic in a voice VLAN in global configuration mode.
voice vlan dscp	Configure the DSCP value for voice traffic in a voice VLAN in global configuration mode.
voice vlan enable	Enable the voice VLAN function on a port.
voice vlan mac-address	Configure a voice traffic OUI to be identified by voice VLAN in global configuration mode.
voice vlan mode auto	Set the voice VLAN of a port to work in automatic mode.
voice vlan security enable	Enable the security mode for a voice VLAN in global configuration mode.

1.1 show voice vlan

Function

Run the **show voice vlan** command to display the configuration and current status of a voice VLAN, including the port on which the voice VLAN function is enabled and the work mode of the voice VLAN.

Syntax

show voice vlan

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the configuration and current status of a voice VLAN on a device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# show voice vlan
Voice VLAN status      : ENABLE
Voice VLAN ID         : 2
Voice VLAN security mode: Security
Voice VLAN aging time   : 5 minutes
Voice VLAN cos        : 6
Voice VLAN dscp       : 46
Current voice vlan enabled port mode:
PORT                            MODE
GigabitEthernet 0/1               Auto
```

Table 1-1 Output Fields of the show voice vlan Command

Field	Description
Voice VLAN status	Whether the voice VLAN function is enabled on a port ● **Enable**: Enabled ● **Disable**: Disabled
Voice VLAN ID	ID of a voice VLAN

Field	Description
Voice VLAN security mode	Security mode of the voice VLAN
Voice VLAN aging time	Aging time of the voice VLAN. The value range is from 5 to 10000, in minutes, and the default value is **1440**.
Voice VLAN cos	Class of Service (CoS) value of voice traffic in the voice VLAN. The value range is from 0 to 7, and the default value is **6**. A larger value indicates a higher priority.
Voice VLAN dscp	Differentiated Services Code Point (DSCP) value of voice traffic in the voice VLAN. The value range is from 0 to 63, and the default value is **46**. A larger value indicates a higher priority.
PORT	Port on which the voice VLAN function is enabled
MODE	Work mode of the port on which the voice VLAN function is enabled

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 show voice vlan oui

Function

Run the **show voice vlan oui** command to display source MAC address entries used by voice VLAN to identify voice packets on the current device.

Syntax

show voice vlan oui

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

You can use this command to display the source MAC address entries used to identify voice packets, including the Organizationally Unique Identifier (OUI), OUI mask, and description.

Examples

The following example displays the source MAC address entries used by voice VLAN to identify voice packets on the current device, including the OUI, OUI mask, and description.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# show voice vlan oui
OUI           Mask          Description
0001.e300.0000  ffff.ff00.0000  Siemensphone
0003.6b00.0000  ffff.ff00.0000  Ciscophone
0004.0d00.0000  ffff.ff00.0000  Avayaphone
0060.b900.0000  ffff.ff00.0000  Philips/NECphone
00d0.1e00.0000  ffff.ff00.0000  Pingtelphone
00e0.7500.0000  ffff.ff00.0000  Polycomphone
00e0.bb00.0000  ffff.ff00.0000  3comphone
```

Table 1-2 Output Fields of the show voice vlan oui Command

Field	Description
OUI	OUI. If the source MAC address in a voice packet matches the OUI, the packet is assigned to the voice VLAN.
Mask	OUI mask, which indicates the valid length of the OUI and is expressed by a mask.
Description	Description of the OUI, which describes the name of a voice device.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 voice vlan

Function

Run the **voice vlan** command to configure an existent common VLAN as a voice VLAN.

Run the **no** form of this command to delete all voice VLANs.

No voice VLAN is configured by default.

Syntax

voice vlan *vlan-id*

no voice vlan

Parameter Description

vlan-id: ID of a voice VLAN. The value range is from 2 to 4094. Only one VLAN can be configured as a voice VLAN on a device.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Caution

- You must create a VLAN before configuring a voice VLAN.
- VLAN 1 is the default VLAN and does not need to be created, but VLAN 1 cannot be configured as a voice VLAN.
- A VLAN cannot be configured as a voice VLAN and a super VLAN at the same time.
- If 802.1x automatic VLAN hopping is enabled on an access port, do not configure the issued VLAN ID as the voice VLAN ID to ensure that 802.1x automatic VLAN hopping functions properly.
- Do not configure a VLAN as a remote VLAN of the remote switched port analyzer (RSPAN) and a voice VLAN at the same time. Otherwise, the RSPAN and voice VLAN functions may be affected.
- Only one voice VLAN can be configured. You must disable the voice VLAN function by running the **no voice vlan** command before you modify the voice VLAN ID.

Examples

The following example creates VLAN 2 and configures VLAN 2 as a voice VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# voice vlan 2
```

Notifications

N/A

Common Errors

See "Usage Guidelines."

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan aging**
- **voice vlan cos**
- **voice vlan dscp**
- **voice vlan enable**
- **voice vlan mac-address**
- **voice vlan mode auto**
- **voice vlan security enable**

1.4 voice vlan aging

Function

Run the **voice vlan aging** command to configure aging time for a port in a voice VLAN in global configuration mode. The aging time indicates the time that the port resides in the voice VLAN when the port fails to receive voice traffic.

Run the **no** form of this command to restore the default configuration.

The default aging time of a port in a voice VLAN is 1440 minutes.

Syntax

voice vlan aging *age*

no voice vlan aging

Parameter Description

age: Aging time of a port in a voice VLAN. The value range is from 5 to 10000, in minutes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can configure the aging time for a port in a voice VLAN on the device. After the MAC address in a voice packet ages, if the device still fails to receive any voice packet from the input port in the specified aging time, the device removes the port from the voice VLAN.

Note

The aging time takes effect in the automatic mode only and starts after the source MAC address in a voice packet ages.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example sets the aging time for a port in a voice VLAN to 10 minutes in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# voice vlan aging 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1.5 voice vlan cos

Function

Run the **voice vlan cos** command to configure the CoS value for voice traffic in a voice VLAN in global configuration mode.

Run the **no** form of this command to restore the default configuration.

The default CoS value of voice traffic in a voice VLAN is **6**.

Syntax

voice vlan cos *cos-value*

no voice vlan cos

Parameter Description

cos-value: CoS value of voice traffic in a voice VLAN. The value range is from 0 to 7. A larger value indicates a higher priority.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can modify the CoS and DSCP values for voice traffic in a voice VLAN on the device to improve the priority of voice traffic and ensure the quality of voice calls.

The CoS value indicates the L2 priority and is saved in the L2 header of a packet. It is filled in the **PRI** field of the IEEE 802.1Q VLAN tag.

The CoS value of a common VLAN packet is **0**, which indicates the lowest priority. The default CoS value of voice traffic in a voice VLAN is **6**, which indicates a higher priority than common VLAN packets.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example sets the CoS value for voice traffic in a voice VLAN to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# voice vlan cos 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1.6 voice vlan dscp

Function

Run the **voice vlan dscp** command to configure the DSCP value for voice traffic in a voice VLAN in global configuration mode.

Run the **no** form of this command to restore the default configuration.

The default DSCP value of voice traffic in a voice VLAN is **46**.

Syntax

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameter Description

dscp-value: DSCP value of voice traffic in a voice VLAN. The value range is from 0 to 63. A larger value indicates a higher priority.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can modify the CoS and DSCP values for voice traffic in a voice VLAN on the device to improve the priority of voice traffic and ensure the quality of voice calls.

The DSCP value indicates the IP priority (IP PRE) and is saved in the L3 header of a packet. For an IPv4 packet, the DSCP value is filled in the first six bits (bit 0 to bit 5) in the **ToS** field of the IPv4 packet header. For an IPv6 packet, the DSCP value is filled in the first six bits in the **Traffic Class** field of the IPv6 packet header.

The DSCP value of a common IP packet is **0**, which indicates the lowest priority. The default DSCP value of voice traffic in a voice VLAN is **46**, which indicates a higher priority than common VLAN packets.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example sets the DSCP value for voice traffic in a voice VLAN to **40**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# voice vlan dscp 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1.7 voice vlan enable

Function

Run the **voice vlan enable** command to enable the voice VLAN function on a port.

Run the **no** form of this command to disable this feature.

The voice VLAN function is disabled on a port by default.

Syntax

voice vlan enable

no voice vlan enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The voice VLAN function must be enabled on a physical port by default. The voice VLAN function can be enabled on an access port, a trunk port, a hybrid port, an uplink port, a host port of PVLAN, and a promiscuous port of PVLAN.

Note

Even if the voice VLAN function is not enabled in global configuration mode, you can also enable the voice VLAN function on a port but the configuration does not take effect.

When a voice VLAN works in automatic mode, the device identifies the source MAC address in a packet and compares the OUI field in the MAC address with the OUI configured on the device. If they match, the device automatically adds the input port of the voice packet to the voice VLAN, issues a policy to change the priority of the voice packet to the voice traffic priority specified for the voice VLAN, and maintains the port in the voice VLAN according to the aging mechanism. Therefore, do not manually add the port to the voice VLAN in automatic mode. Ensure that the voice VLAN is not in the allowed VLAN list of the port. Otherwise, the voice VLAN function cannot be enabled on the port.

When a voice VLAN works in manual mode, you are required to manually add the port to the voice VLAN and then enable the voice VLAN function on the port. The device identifies the source MAC address in a packet and compares the OUI field in the MAC address with the OUI configured on the device. If they match, the device delivers a policy to change the priority of the voice packet to the voice traffic priority specified for the voice VLAN.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example connects a PC and a VoIP telephone to GigabitEthernet 0/1 in serial mode. In this case, the voice VLAN works in automatic mode. VLAN 5 is created to transmit PC data traffic, and VLAN 2 is created as a voice VLAN to transmit voice traffic. GigabitEthernet 0/1 is configured as a trunk port, VLAN 5 is added to the allowed VLAN list of the port, voice VLAN 2 is excluded from the VLAN list, and the voice VLAN function is enabled on GigabitEthernet 0/1.

The voice VLAN function must be enabled on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 5
```

```
Hostname(config-vlan)# exit
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# voice vlan 2
Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 5
Hostname(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan remove 2
Hostname(config-if-GigabitEthernet 0/1)# voice vlan mode auto
Hostname(config-if-GigabitEthernet 0/1)# voice vlan enable
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# voice vlan aging 10
Hostname(config)# voice vlan security enable
Hostname(config)# voice vlan cos 7
Hostname(config)# voice vlan dscp 47
```

The following example connects only a VoIP telephone to GigabitEthernet 0/1. In this case, the voice VLAN can be set to work in manual mode; VLAN 2 is created and VLAN 2 is configured as a voice VLAN; the port is added to voice VLAN 2 and the voice VLAN function is enabled on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# voice vlan 2
Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode access
Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 2
Hostname(config-if-GigabitEthernet 0/1)# no voice vlan mode auto
Hostname(config-if-GigabitEthernet 0/1)# voice vlan enable
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# voice vlan security enable
Hostname(config)# voice vlan cos 7
Hostname(config)# voice vlan dscp 47
```

Notifications

A port is configured to work in voice VLAN automatic mode but the voice VLAN is contained in the allowed VLAN list of the port. When you try to enable the voice VLAN function on the port, the following notification will be displayed:

```
Can't enable voice VLAN because the port is in voice VLAN and auto mode has been set.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1.8 voice vlan mac-address

Function

Run the **voice vlan mac-address** command to configure a voice traffic OUI to be identified by voice VLAN in global configuration mode.

Run the **no** form of this command to remove this configuration.

No OUI of any voice device is configured by default.

Syntax

voice vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

no voice vlan mac-address *mac-address*

Parameter Description

mac-address: Source MAC address in a voice packet. This field follows the format of *H.H.H*.

mask *oui-mask*: Valid length of an OUI, which is expressed by a mask. This field follows the format of *H.H.H*.

description *text*: Description of an OUI.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A voice device identifies a vendor according to the first three bytes of the MAC address. Voice VLAN perform the logical "AND" operation on the source MAC address in a received packet and the OUI mask to obtain the OUI of the packet transmission device, so as to judge whether the packet is a voice packet.

The voice VLAN OUI cannot be a multicast address, and the configured mask should not contain non-consecutive 1's.

You can use the **show voice vlan oui** command to display the OUI for identifying a packet as a voice packet on the current device, OUI mask, and description.

Examples

The following example sets the voice traffic OUI to be identified by voice VLAN to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to Company-A in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company-A
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan oui**
- **voice vlan**

1.9 voice vlan mode auto

Function

Run the **voice vlan mode auto** command to set the voice VLAN of a port to work in automatic mode.

Run the **no** form of this command to set the voice VLAN of a port to work in manual mode.

By default, the voice VLAN of a port works in automatic mode.

Syntax

voice vlan mode auto

no voice vlan mode auto

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The voice VLAN can work in automatic mode or manual mode, depending on the port configuration. The voice VLAN work modes of ports are independent of each other. Different voice VLAN work modes can be configured for different ports. The methods of adding ports to voice VLANs vary with the work mode. You can configure the voice VLAN work mode of a port based on the type of VoIP telephone connected to the port and the port type.

Caution

- If the voice VLAN function is enabled on a port and the voice VLAN works in manual mode, you must manually add the port to the voice VLAN to ensure that the voice VLAN function can take effect.
- If the voice VLAN on a port works in automatic mode, the device automatically adds the port to the voice VLAN. Do not configure the native VLAN of the port as a voice VLAN. Remove the voice VLAN from the allowed static VLAN list of the port before enabling the voice VLAN in automatic mode. After the automatic

mode is enabled, you are not allowed to add the port to or remove the port from the voice VLAN by running the **switchport trunk allowed vlan remove 2** command.

- The trunk or hybrid port of this device can transmit packets of all VLANs by default. You need to remove the voice VLAN from the allowed static VLAN list of the port and then enable the voice VLAN function. The purpose is to ensure that ports not connected to voice devices will not be added to the voice VLAN and the ports left unused for a long time will not stay in the voice VLAN.
- After the voice VLAN function is enabled on a port, you are not allowed to manually switch the port between the manual mode and automatic mode. To change the voice VLAN work mode, you must first disable the voice VLAN function on the port.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example connects a PC and a VoIP telephone to GigabitEthernet 0/1 in serial mode. In this case, the voice VLAN works in automatic mode. VLAN 5 is created to transmit PC data traffic, and VLAN 2 is created as a voice VLAN to transmit voice traffic. GigabitEthernet 0/1 is configured as a trunk port.

(1) The following example sets the MAC address for identifying voice packets to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to Company A in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company A
```

(2) The following example creates VLAN 5 to transmit data traffic and creates VLAN 2 as a voice VLAN to transmit voice traffic.

```
Hostname(config)# vlan 5
Hostname(config-vlan)# exit
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# voice vlan 2
```

(3) The following example configures GigabitEthernet 0/1 as a trunk port, configures VLAN 5 as the native VLAN, and removes voice VLAN 2 from the allowed static VLAN list of the port.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 5
Hostname(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan remove 2
```

(4) The following example sets the voice VLAN of the port to work in automatic mode. When the port receives a packet with the MAC address matching the voice VLAN OUI, the port automatically adds the voice VLAN to the allowed VLAN list of the port and forwards the voice packet over the voice VLAN.

```
Hostname(config-if-GigabitEthernet 0/1)# voice vlan mode auto
```

(5) The following example enables the voice VLAN function on the port.

```
Hostname(config-if-GigabitEthernet 0/1)# voice vlan enable
Hostname(config-if-GigabitEthernet 0/1)# exit
```

Notifications

When you configure a voice VLAN to work in automatic mode and then try to change the allowed VLAN list of the port, the following notification will be displayed.

```
Can't change allowed VLAN since voice VLAN has been enabled and auto mode has been set.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1.10 voice vlan security enable

Function

Run the **voice vlan security enable** command to enable the security mode for a voice VLAN in global configuration mode.

Run the **no** form of this command to disable the security mode of the voice VLAN and restore the voice VLAN to the common mode.

The security mode of a voice VLAN is enabled by default, that is, the voice VLAN works in security mode.

Syntax

voice vlan security enable

no voice vlan security enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To better isolate voice traffic from data traffic during transmission, you can enable the security mode of a voice VLAN. After the security mode is enabled, the device checks the source MAC address in each packet. When the source MAC address in the packet matches the OUI of the voice VLAN, the device allows this packet to be transmitted over the voice VLAN. Otherwise, the device discards this packet.

Caution

Do not transmit voice data and service data over the voice VLAN at the same time. If you want to transmit both voice data and service data over the voice VLAN, confirm that the security mode of the voice VLAN function is disabled.

Note

In security mode, the device checks the source MAC addresses of only untagged packets and packets with a voice VLAN tag. For packets with non-voice VLAN tags, the device forwards or discards these packets according to the common VLAN rules, irrespective of the security mode of the voice VLAN.

You can run the **show voice vlan** command to display the configuration and current status of a voice VLAN.

Examples

The following example disables the security mode of a voice VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no voice vlan security enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show voice vlan**
- **voice vlan**

1 GVRP Commands

Command	Function
bridge-frame forwarding protocol gvrp	Enable the transparent transmission function of packets of Generic Attribute Registration Protocol (GARP) VLAN registration protocol (GVRP) bridge protocol data unit (BPDU).
clear gvrp statistics	Clear the statistics of GVRP and restart counting.
gvrp applicant state	Configure the advertising mode of a port.
gvrp dynamic-vlan-creation enable	Enable the function of creating virtual local area network (VLAN) dynamically.
gvrp enable	Enable the GVRP function.
gvrp registration mode	Configure the registration mode of a port.
gvrp timer	Configure the GVRP timer.
l2protocol-tunnel gvrp	Enable the GVRP BPDU tunnel function globally.
l2protocol-tunnel gvrp enable	Enable the GVRP BPDU tunnel function on a port.
l2protocol-tunnel gvrp tunnel-dmac	Configure the tunnel address for transmitting the user's GVRP BPDU.
show gvrp configuration	Display the GVRP configuration.
show gvrp statistics	Display the GVRP statistics.
show gvrp status	Display the GVRP port information.
show l2protocol-tunnel gvrp	Display the configuration of a GVRP BPDU tunnel.

1.1 bridge-frame forwarding protocol gvrp

Function

Run the **bridge-frame forwarding protocol gvrp** command to enable the transparent transmission function of packets of Generic Attribute Registration Protocol (GARP) VLAN registration protocol (GVRP) bridge protocol data unit (BPDU).

Run the **no** form of this command to disable the transparent transmission function of GVRP BPDU packets.

The transparent transmission function of GVRP BPDU packets is disabled by default.

Syntax

bridge-frame forwarding protocol gvrp

no bridge-frame forwarding protocol gvrp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

According to the IEEE 802.1Q standard, GVRP BPDU uses the dedicated address 0180.c200.0021 as the destination MAC address; the device compliant with the IEEE 802.1Q standard will not forward the packets with the destination MAC address 0180.c200.0021. However, in the actual network deployment, devices are required to transparently transmit GVRP BPDU packets in some cases. For example, when GVRP is disabled for a device, GVRP BPDU packets need to be transparently transmitted so that another device interconnected to such a device through GVRP BPDU can normally calculate the GVRP topology.

GVRP transparent transmission takes effect only when GVRP is disabled. If GVRP is enabled, devices do not transparently transmit GVRP BPDU packets.

Examples

The following example enables the transparent transmission function of GVRP BPDU packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bridge-frame forwarding protocol gvrp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear gvrp statistics

Function

Run the **clear gvrp statistics** command to clear the statistics of GVRP and restart counting.

Syntax

clear gvrp statistics { *interface-type interface-number* | **all** }

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example clears the statistics of GVRP and restarts counting.

```
Hostname> enable
Hostname# clear gvrp statistics all
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**
- **show gvrp status**

1.3 gvrp applicant state

Function

Run the **gvrp applicant state** command to configure the advertising mode of a port.

Run the **no** form of this command to restore the default configuration.

The advertising mode of a port is **normal** by default.

Syntax

gvrp applicant state { **normal** | **non-applicant** }

no gvrp applicant state

Parameter Description

normal: Allows a port to externally send GVRP advertisements to advertise VLAN messages.

non-applicant: Not allows a port to externally send GVRP advertisements to advertise VLAN messages.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the GVRP advertising mode of a port as **normal**, namely, GVRP advertisements are sent externally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# gvrp enable
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# gvrp applicant state normal
```

Notifications

When the command is configured for a port not in the trunk mode, the following notification will be displayed:

```
It isn't a trunk port; the GVRP applicant type can't be specified.
```

When you try to configure the GVRP advertising mode but do not enable the GVRP function using the **gvrp enable** command in advance, the following notification will be displayed:

```
GVRP is disabled globally. GVRP status of port cannot be changed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**
- **show l2protocol-tunnel gvrpshow l2protocol-tunnel gvrp**

- **show gvrp configuration**

1.4 gvrp dynamic-vlan-creation enable

Function

Run the **gvrp dynamic-vlan-creation enable** command to enable the function of creating virtual local area network (VLAN) dynamically.

Run the **no** form of this command to disable this feature.

The function of creating VLANs dynamically is disabled by default.

Syntax

gvrp dynamic-vlan-creation enable

no gvrp dynamic-vlan-creation enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of creating VLANs dynamically.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# gvrp dynamic-vlan-creation enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**
- **show l2protocol-tunnel gvrp**
- **show gvrp configuration**

1.5 gvrp enable

Function

Run the **gvrp enable** command to enable the GVRP function.

Run the **no** form of this command to disable the GVRP function.

The GVRP function is disabled by default.

Syntax

gvrp enable

no gvrp enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the GVRP function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# gvrp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show l2protocol-tunnel gvrp**
- **show gvrp configuration**

1.6 gvrp registration mode

Function

Run the **gvrp registration mode** command to configure the registration mode of a port.

Run the **no** form of this command to restore the default configuration.

The registration mode of a port is **disable** by default.

Syntax

gvrp registration mode { **normal** | **disable** }

no gvrp registration mode

Parameter Description

normal: Allows dynamic creation, registration, or deregistration of VLAN on a port.

disable: Not allows dynamic creation, registration, or deregistration of VLAN on a port.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example configures the registration mode of a port as **normal**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# gvrp enable
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# gvrp registration mode normal
```

Notifications

When the command is configured for a port not in the trunk mode, the following notification will be displayed:

```
It isn't a trunk port; the GVRP applicant type can't be specified.
```

When the GVRP function is not enabled globally using the **gvrp enable** command and you try to configure the GVRP registration mode, the following notification will be displayed:

```
GVRP is disabled globally. GVRP status of port cannot be changed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**
- **show l2protocol-tunnel gvrp**
- **show gvrp configuration**

1.7 gvrp timer

Function

Run the **gvrp timer** command to configure the GVRP timer.

Run the **no** form of this command to restore the default configuration.

By default, the maximum delay before a port sends a join or leave message is 200 ms, the waiting time from receiving a leave message by the port to deleting the port from the VLAN is 600 ms, and the minimum time interval for the port to send a LeaveAll message is 10,000 ms.

Syntax

gvrp timer { **join** *hold* | **leave** *leave* | **leaveall** *leaveall* }

no gvrp timer

Parameter Description

join *hold*: Configures the maximum delay before a port sends a join or leave message in milliseconds. The value range is from 1 to 200, and the default value is 200. The actual sending interval is in the range from 0 to *hold*.

leave *leave*: Configures the waiting time from receiving a leave message by the port to deleting the port from the VLAN in milliseconds. The value range is from 600 to 9999, and the default value is 600. If the port receives a join message again in this period, the port will not be deleted from the VLAN and the timer will expire; if the join message is not received before the timer times out, the state of the port changes to **Empty** and the port is deleted from the VLAN member list.

leaveall *leaveall*: Configures the minimum time interval for the port to send a LeaveAll message in milliseconds. The value range is from （ *leave*+1 ） to 2147483647, and the default value is 10000. If the port timer times out, the LeaveAll message is sent, and the actual sending interval ranges from *leaveall* to the sum of *leaveall* and *hold*; the LeaveAll message is also sent to the local port to trigger the Leave timer to start counting; if the port receives the LeaveAll message before the timer times out, the timer restarts timing.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

The three timers are subject to this relationship: 3 x Hold ≤ Leave ≤ LeaveAll.

Examples

The following example sets the maximum delay before the GVRP port sends an advertisement to 300 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# gvrp timer join 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**
- **show l2protocol-tunnel gvrp**
- **show gvrp configuration**

1.8 l2protocol-tunnel gvrp

Function

Run the **l2protocol-tunnel gvrp** command to enable the GVRP BPDU tunnel function globally.

Run the **no** form of this command to disable the GVRP BPDU tunnel function globally.

The global GVRP BPDU tunnel function is disabled by default.

Syntax

l2protocol-tunnel gvrp

no l2protocol-tunnel gvrp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

To enable the global GVRP BPDU tunnel function, please also enable the GVRP BPDU tunnel function on the port.

Examples

The following example enables the GVRP BPDU tunnel function globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel gvrp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show l2protocol-tunnel gvrp**

1.9 l2protocol-tunnel gvrp enable

Function

Run the **l2protocol-tunnel gvrp enable** command to enable the GVRP BPDU tunnel function on a port.

Run the **no** form of this command to disable the GVRP BPDU tunnel function on a port.

The GVRP BPDU tunnel function on a port is disabled by default.

Syntax

l2protocol-tunnel gvrp enable

no l2protocol-tunnel gvrp enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

The GVRP BPDU tunnel function takes effect only when it is enabled globally and on the port at the same time.

Examples

The following example enables the GVRP BPDU tunnel function globally. The following example enables the GVRP BPDU tunnel function on a port.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel gvrp
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# l2protocol-tunnel gvrp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show l2protocol-tunnel gvrp**

1.10 l2protocol-tunnel gvrp tunnel-dmac

Function

Run the **l2protocol-tunnel gvrp tunnel-dmac** command to configure the tunnel address for transmitting the user's GVRP BPDU.

Run the **no** form of this command to restore the default configuration.

The default tunnel address for transmitting the user's GVRP BPDU is 01d0.f800.0006.

Syntax

l2protocol-tunnel gvrp tunnel-dmac *gvrp-dmac-address*

no l2protocol-tunnel gvrp tunnel-dmac

Parameter Description

gvrp-dmac-address: Tunnel address for transmitting GVRP packets of the user network. The value range is from 01d0.f800.0006 and 011a.a900.0006, and the default value is 01d0.f800.0006.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

To avoid impact on the SP network by GVRP packets of the user network, when GVRP packets of the user network enter an edge device of the SP network, the edge device changes the destination MAC address of the packets from the GVRP dedicated address (0180.c200.0006) to the tunnel address (01d0.f800.0006 by default) before forwarding on the SP network. After the packets are forwarded to an edge device at the other end, the destination MAC address is restored from the tunnel address (01d0.f800.0006 by default) to the GVRP

dedicated address (0180.c200.0006), and the packets are forwarded to the user network at the other end. In this way, the GVRP packets of the user network are transmitted through the tunnel of the SP network.

Examples

The following example sets the tunnel address for transmitting the user's GVRP BPDU to 011a.a900.0006.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006
```

Notifications

When the configured GVRP tunnel address is not in the above address range, the following notification will be displayed:

```
Optional at the following addresses: 01d0.f800.0006,011a.a900.0006.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show l2protocol-tunnel gvrp**

1.11 show gvrp configuration

Function

Run the **show gvrp configuration** command to display the GVRP configuration.

Syntax

show gvrp configuration

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the GVRP configuration.

```
Global GVRP Configuration:
```

```
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
----------------------  ----------------------  ----------------------
GigabitEthernet 0/2          normal                 normal
```

Table 1-1 Output Fields of the show gvrp configuration Command

Field	Description
GVRP Feature	Indicates whether GVRP is enabled.
GVRP dynamic VLAN creation	Indicates whether the function of creating VLANs dynamically is enabled.
Join Timers	Indicates the time of the Join timer.
Leave Timers	Indicates the time of the Leave timer.
Leaveall Timers	Indicates the time of the LeaveAll timer.
PORT	Indicates the port.
Applicant Status	Indicates the advertising mode.
Registration Mode	Indicates the registration mode.

Notifications

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**

1.12 show gvrp statistics

Function

Run the **show gvrp statistics** command to display the GVRP statistics.

Syntax

show gvrp statistics { *interface-type interface-number* | **all** }

Parameter Description

interface-type interface-number: GVRP statistics of the specified port.

all: Displays the GVRP statistics of all the ports.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the GVRP statistics of the port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show gvrp statistics gigabitethernet 0/1
Interface      GigabitEthernet 0/1
RecValidGvrpPdu        0
RecInvalidGvrpPdu      0
RecJoinEmpty    0
RecJoinIn      0
RecEmpty       0
RecLeaveEmpty   0
RecLeaveIn     0
RecLeaveAll    0
SentGvrpPdu    0
SentJoinEmpty   0
SentJoinIn     0
SentEmpty      0
SentLeaveEmpty  0
SentLeaveIn    0
SentLeaveAll   0
JoinIndicated   0
LeaveIndicated  0
JoinPropagated  0
LeavePropagated  0
```

Table 1-2 Output Fields of the show gvrp statistics Command

Field	Description
RecValidGvrpPdu	Indicates the number of received valid GPDU packets.
RecInvalidGvrpPdu	Indicates the number of received invalid GPDU packets.
RecJoinEmpty/ SentJoinEmpty	Indicates the number of received/sent JoinEmpty messages.
RecJoinIn/ SentJoinIn	Indicates the number of received/sent JoinIn messages.
RecEmpty/SentEmpty	Indicates the number of received/sent Empty messages.

Field	Description
RecLeaveEmpty/SentLeaveEmpty	Indicates the number of received/sent LeaveEmpty messages.
RecLeaveIn/ SentLeaveIn	Indicates the number of received/sent LeaveIn messages.
RecLeaveAll/SentLeaveAll	Indicates the number of received/sent LeaveAll messages.
SentGvrpPdu	Indicates the total number of sent GPDU messages.
JoinIndicated/ LeaveIndicated	Indicates the number of Join/Leave service requests.
JoinPropagated / LeavePropagated	Indicates the number of Join/Leave topology update requests.

Notifications

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**

1.13 show gvrp status

Function

Run the **show gvrp status** command to display the GVRP port information.

Syntax

show gvrp status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display the GVRP port information of all member ports in a dynamic VLAN and the GVRP port information of dynamic member ports in a static VLAN.

Examples

The following example displays the GVRP information.

```
Hostname> enable
```

```
Hostname# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 2
Dynamic Ports:
```

Table 1-3 Output Fields of the show gvrp status Command

Field	Description
VLAN	Indicates a static VLAN.
DVLAN	Indicates a dynamic VLAN.
Dynamic Ports	Indicates dynamic member ports.

Notifications

N/A

Platform Description

N/A

Related Commands

- **gvrp enable**

1.14 show l2protocol-tunnel gvrp

Function

Run the **show l2protocol-tunnel gvrp** command to display the configuration of a GVRP BPDU tunnel.

Syntax

show l2protocol-tunnel gvrp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the configuration of a GVRP BPDU tunnel.

```
Hostname> enable
Hostname# show l2protocol-tunnel gvrp
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address:011a.a900.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel gvrp**
- **l2protocol-tunnel gvrp enable**

1 QinQ Commands

Command	Function
dot1q outer-vid register inner-vid	Configure a policy of adding an outer VID based on the inner VID of packets.
dot1q-tunnel cos remark-cos	Configure a priority mapping policy and modify the outer priority based on the inner priority of input packets.
frame-tag tpid	Configure TPID of packets.
inner-priority-trust enable	Configure a priority replication policy and replicate the inner priority of input packets as outer priority.
l2protocol-tunnel	Enable the layer-2 protocol tunneling function globally.
l2protocol-tunnel enable	Enable the layer-2 protocol tunneling function on an interface.
l2protocol-tunnel tunnel-dmac	Configure a layer-2 protocol tunnel address.
show dot1q-tunnel	Display the dot1q-tunnel configuration of an interface.
show frame-tag tpid	Display the TPID configuration of an interface.
show inner-priority-trust	Display the priority replication configuration of an interface.
show interfaces dot1q-tunnel	Display the configuration of allowed VLANs and native VLANs of a dot1q-tunnel port.
show interfaces remark	Display the priority mapping configuration of an interface.
show l2protocol-tunnel	Display the configuration of layer-2 protocol transparent transmission.
show registration-table	Display the policy of adding the outer VID based on the inner VID of packets.
show translation-table	Display the inner and outer VID modification policy.
switchport dot1q-tunnel allowed vlan	Configure allowed VLANs of the dot1q-tunnel port.
switchport dot1q-tunnel native vlan	Configure the native VLAN of dot1q-tunnel.

switchport mode dot1q-tunnel	Configure an interface as a dot1q-tunnel port.

1.1 dot1q outer-vid register inner-vid

Function

Run the **dot1q outer-vid register inner-vid** command to configure a policy of adding an outer VID based on the inner VID of packets.

Run the **no** form of this command to delete a policy of adding an outer VID based on the inner VID of packets.

Run the **default** form of this command to restore the default configuration.

No policy of adding an outer VID based on the inner VID of packets is configured by default.

Syntax

dot1q outer-vid *svid* **register inner-vid** *cvid-list*

no dot1q outer-vid *svid* **register inner-vid** *cvid-list*

default dot1q outer-vid *svid* **register inner-vid** *cvid-list*

Parameter Description

svid: Outer VLAN ID added for input packets. It is a VLAN ID of the SP network, and the value range is from 1 to 4094.

cvid-list: Inner VLAN ID list of input packets, which can include one or more VLANs. When multiple VLANs are included, they are separated by commas. You can also specify a VLAN range by connecting the start VLAN ID and end VLAN ID using an en dash (–). It contains VLAN IDs of the client network, and the value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a C-Tag-based QinQ encapsulation policy. It can be configured only on the dot1q-tunnel and hybrid ports.

You can run the **show registration-table** [**interface** *interface-type interface-number*] command to display the related configuration on the interface.

Examples

The following example adds the outer VID 30 on the dot1q-tunnel port GigabitEthernet 0/1 when the inner VID of input packets ranges from 11 to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 30
Hostname(config-vlan)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
```

```
Hostname(config-if-GigabitEthernet 0/1)# dot1q outer-vid 30 register inner-vid 11-20
```

The following example adds the outer VLAN ID 10 on the hybrid port GigabitEthernet 0/2 when the inner VID of input packets ranges from 1 to 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 10
Hostname(config-vlan)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/2)# dot1q outer-vid 10 register inner-vid 1-10
```

Notifications

If this command is configured when the destination VLAN is not created in advance, the following notification will be displayed:

```
The destination vlan 30 shall be exist,undynamic and not supervlan.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport mode dot1q-tunnel**
- **show registration-table**

1.2 dot1q-tunnel cos remark-cos

Function

Run the **dot1q-tunnel cos remark-cos** command to configure a priority mapping policy and modify the outer priority based on the inner priority of input packets.

Run the **no** form of this command to delete a priority mapping policy.

Run the **default** form of this command to restore the default configuration.

No policy of mapping the outer priority based on the inner priority of input packets is configured by default.

Syntax

dot1q-tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

no dot1q-tunnel cos *inner-cos-value* **remark-cos**

default dot1q-tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

Parameter Description

inner-cos-value: Inner priority of input packets. The value range is from 0 to 7. A larger value indicates a higher priority.

outer-cos-value: Outer priority of input packets. The value range is from 0 to 7. A larger value indicates a higher priority.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When a priority mapping policy is configured, the CoS value of the outer tag can be set to different values based on the packet priority. In this case, important services can be preferentially transmitted and processed.

You can run the **show interface** [**interface** *interface-type interface-number*] **remark** command to display the related configuration on the interface.

Examples

The following example configures a priority mapping policy on the dot1q-tunnel port GigabitEthernet 0/1, and maps the CoS value of outer VLAN tag priority to 5 when the CoS value of inner VLAN tag priority of input packets is 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-GigabitEthernet 0/1)# dot1q-Tunnel cos 3 remark-cos 5
```

Notifications

When the interface is not configured as the dot1q-tunnel mode and priority mapping configuration is not supported, the following notification will be displayed:

```
Only support the tunnel-mode switchport.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show interfaces remark**

1.3 frame-tag tpid

Function

Run the **frame-tag tpid** command to configure TPID of packets.

Run the **no** form of this command to delete the configured TPID value and restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default TPID value is 0x8100.

Syntax

frame-tag tpid *tpid*

no frame-tag tpid

default frame-tag tpid

Parameter Description

tpid: Packet type value. The value range is from 0 to ffff in hexadecimal. The common value is 0x8100 or 0x9100. The default value 0x8100 indicates IEEE 802.1Q frame.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the TPID value of a third-party device is not the default value 0x8100 defined in IEEE 802.1Q, the TPID value needs to be configured on the port connected to the third-party device to keep consistency and compatibility with the third-party device.

Run the **show frame-tag tpid** command to display the configuration.

Examples

The following example sets the packet type value to 0x9100 on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# frame-tag tpid 0x9100
```

Notifications

When no TPID value is displayed, the following notification will be displayed, indicating that TPID is the default value 0x8100:

```
Hostname# show frame-tag tpid
Ports   tpid
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show frame-tag tpid**

1.4 inner-priority-trust enable

Function

Run the **inner-priority-trust enable** command to configure a priority replication policy and replicate the inner priority of input packets as outer priority.

Run the **no** form of this command to delete the priority replication policy.

Run the **default** form of this command to restore the default priority.

The priority replication function is disabled by default.

Syntax

inner-priority-trust enable

no inner-priority-trust enable

default inner-priority-trust enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a priority replication policy is configured, the client VLAN tag priority can be replicated to the outer VLAN tag priority so that the client packets are encapsulated with the outer VLAN tag and have the same priority as the client VLAN tag. In this case, the client packets can be preferentially processed and transmitted in the SP network.

Run the **show inner-priority-trust** command to display the configuration.

Examples

The following example configures a priority replication policy and replicates the inner tag priority of input packets of the interface GigabitEthernet 0/1 as the outer tag priority.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-gigabitethernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-gigabitethernet 0/1)# inner-priority-trust enable
```

Notifications

When the interface is not configured as the dot1q-tunnel mode and priority replication configuration is not supported, the following notification will be displayed:

```
Only support the tunnel-mode switchport.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show inner-priority-trust**

1.5 l2protocol-tunnel

Function

Run the **l2protocol-tunnel** command to enable the layer-2 protocol tunneling function globally.

Run the **no** form of this command to disable the layer-2 protocol tunneling function globally.

Run the **default** form of this command to restore the default configuration.

The layer-2 protocol tunneling function is disabled globally by default.

Syntax

l2protocol-tunnel { **stp** | **gvrp** }

no l2protocol-tunnel { **stp** | **gvrp** }

default l2protocol-tunnel { **stp** | **gvrp** }

Parameter Description

stp: Enables a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) tunnel.

gvrp: Enables a GARP VLAN registration protocol (GVRP) BPDU tunnel.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The layer-2 protocol tunneling function takes effect only when it is enabled globally and on the interface at the same time.

You can run the **show l2protocol-tunnel** { **gvrp** | **stp** } command display the configuration.

Examples

The following example enables the layer-2 protocol (GVRP and STP) tunneling function globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# l2protocol-tunnel gvrp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bridge-frame forwarding protocol bpdu**
- **l2protocol-tunnel enable**
- **show l2protocol-tunnel**

1.6 l2protocol-tunnel enable

Function

Run the **l2protocol-tunnel enable** command to enable the layer-2 protocol tunneling function on an interface.

Run the **no** form of this command to disable the layer-2 protocol tunneling function on an interface.

Run the **default** form of this command to restore the default configuration.

The layer-2 protocol tunneling function is disabled on an interface by default.

Syntax

l2protocol-tunnel { **stp** | **gvrp** } **enable**

no l2protocol-tunnel { **stp** | **gvrp** } **enable**

default l2protocol-tunnel { **stp** | **gvrp** } **enable**

Parameter Description

stp: Enables the STP BPDU tunneling function.

gvrp: Enables the GVRP BPDU tunneling function.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The layer-2 protocol tunneling function takes effect only when it is enabled globally and on the interface at the same time.

You can run the **show l2protocol-tunnel** { **gvrp** | **stp** } command to display the configuration.

Examples

The following example enables the layer-2 protocol STP BPDU tunneling function on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-GigabitEthernet 0/1)# l2protocol-tunnel stp enable
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# l2protocol-tunnel stp
```

The following example enables the layer-2 protocol GVRP BPDU tunneling function on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-GigabitEthernet 0/1)# l2protocol-tunnel gvrp enable
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# l2protocol-tunnel gvrp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel**
- **bridge-frame forwarding protocol bpdu**
- **show l2protocol-tunnel**

1.7 l2protocol-tunnel tunnel-dmac

Function

Run the **l2protocol-tunnel tunnel-dmac** command to configure a layer-2 protocol tunnel address.

Run the **no** form of this command to delete the layer-2 protocol tunnel address.

Run the **default** form of this command to restore the default configuration.

The default BPDU tunnel address of STP packets is 01d0.f800.0005, and that of GVRP packets is 01d0.f800.0006.

Syntax

l2protocol-tunnel { **stp** | **gvrp** } **tunnel-dmac** *mac-address*

no l2protocol-tunnel { **stp** | **gvrp** } **tunnel-dmac** *mac-address*

default l2protocol-tunnel { **stp** | **gvrp** } **tunnel-dmac** *mac-address*

Parameter Description

stp *mac-address*: Configures the BPDU tunnel address of STP packets. The value is 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, or 0100.0ccd.cdd2.

gvrp *mac-address*: Configures the BPDU tunnel address of GVRP packets. The value is 01d0.f800.0006 or 011a.a900.0006.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **show l2protocol-tunnel** { **gvrp** | **stp** } command to display the configuration.

Examples

The following example sets the BPDU tunnel address of layer-2 protocol (GVRP) to 011a.a900.0006 globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show l2protocol-tunnel**

1.8 show dot1q-tunnel

Function

Run the **show dot1q-tunnel** command to display the dot1q-tunnel configuration of an interface.

Syntax

show dot1q-tunnel [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface of which the dot1q-tunnel configuration will be displayed. If this parameter is not specified, the dot1q-tunnel configuration of all interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the dot1q-tunnel configuration of all interfaces.

```
Hostname> enable
Hostname# show dot1q-tunnel
Ports  Dot1q-tunnel
-----  ------------
Gi0/1  Enable
Gi0/2  disable
```

Table 1-1 Output Fields of the show dot1q-tunnel Command

Field	Description
Ports	Indicates the interface name.
Dot1q-tunnel	Indicates the configuration status of dot1q-tunnel function: ● **Enable**: Indicates that the function is enabled. ● **Disable**: Indicates that the function is disabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show frame-tag tpid

Function

Run the **show frame-tag tpid** command to display the TPID configuration of an interface.

Syntax

show frame-tag tpid [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface of which the TPID configuration will be displayed. If this parameter is not specified, the TPID configuration of all interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the TPID configuration of all interfaces.

```
Hostname> enable
Hostname# show frame-tag tpid
Ports    Tpid
------   --------
Gi0/1    0x9100
```

Table 1-2 Output Fields of the show frame-tag tpid Command

Field	Description
Ports	Indicates the interface name.
tpid	Indicates the TPID value.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show inner-priority-trust

Function

Run the **show inner-priority-trust** command to display the priority replication configuration of an interface.

Syntax

show inner-priority-trust [**interfaces** *interface-type interface-number*]

Parameter Description

interfaces *interface-type interface-number*: Specifies the interface of which the priority replication function will be displayed. If this parameter is not specified, the priority replication configuration of all the interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the priority replication configuration of all interfaces.

```
Hostname> enable
Hostname# show inner-priority-trust
Ports        Inner-priority-trust
------------  ----------
Gi0/1        Disable
Gi0/2        Enable
Gi0/3        Disable
Gi0/4        Disable
```

Table 1-3 Output Fields of the show inner-priority-trust Command

Field	Description
Ports	Indicates the interface name.
inner-priority-trust	Indicates whether priority replication is enabled on the interface: ● **Enable**: Indicates that the function is enabled. ● **Disable**: Indicates that the function is disabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show interfaces dot1q-tunnel

Function

Run the **show interfaces dot1q-tunnel** command to display the configuration of allowed VLANs and native VLANs of a dot1q-tunnel port.

Syntax

show interfaces [*interface-type interface-number*] **dot1q-tunnel**

Parameter Description

interface-type interface-number: Specifies the dot1q-tunnel port of which the configuration of allowed VLANs and native VLANs will be displayed. If this parameter is not specified, the configuration of allowed VLANs and native VLANs of all dot1q-tunnel ports will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the configuration of allowed VLANs and native VLANs of all dot1q-tunnel ports.

```
Hostname> enable
Hostname# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:
```

Table 1-4 Output Fields of the show interfaces dot1q-tunnel Command

Field	Description
Interface	Indicates the interface name.
Native vlan	Indicates the native VLAN of the interface.
Allowed vlan list	Indicates the list of VLANs that packets are allowed to pass through.
Tagged vlan list	Indicates the list of VLANs where the output packets carry tags.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show interfaces remark

Function

Run the **show interfaces remark** command to display the priority mapping configuration of an interface.

Syntax

show interfaces [*interface-type interface-number*] **remark**

Parameter Description

interface-type interface-number: Specifies the interface of which the priority mapping configuration will be displayed. If this parameter is not specified, the priority mapping configuration of all interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the priority mapping configuration of all interfaces.

```
Hostname> enable
Hostname# show interfaces remark
Ports       From COS   To COS
----------- ---------- ----------
Gi0/1       3          5
Gi0/2       4          2
```

Table 1-5 Output Fields of the show interfaces remark Command

Field	Description
Ports	Indicates the interface name.

Field	Description
Type	Indicates the type of priority mapping.
From value	Indicates the priority of the inner tag.
To value	Indicates the priority of the outer tag.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show l2protocol-tunnel

Function

Run the **show l2protocol-tunnel** command to display the configuration of layer-2 protocol transparent transmission.

Syntax

show l2protocol-tunnel { **gvrp** | **stp** }

Parameter Description

gvrp: Displays the configuration of a GVRP BPDU tunnel.

stp: Displays the configuration of an STP BPDU tunnel.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the configuration of STP transparent transmission.

```
Hostname> enable
Hostname# show l2protocol-tunnel stp
L2protocol-tunnel: stp Disable
L2protocol-tunnel destination mac address: 01d0.f800.0005
```

The following example displays the configuration of GVRP transparent transmission.

```
Hostname> enable
Hostname# show l2protocol-tunnel gvrp
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address:01d0.f800.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
GigabitEthernet 0/2 l2protocol-tunnel gvrp enable
```

Table 1-6 Output Fields of the show l2protocol-tunnel Command

Field	Description
L2protocol-tunnel	Indicates the enabling status of layer-2 protocol tunneling. ● **Enable**: Indicates that layer-2 protocol tunneling is enabled. ● **Disable**: Indicates that layer-2 protocol tunneling is disabled.
L2protocol-tunnel destination mac address	Indicates the MAC address of layer-2 protocol tunneling.
l2protocol-tunnel gvrp enable	Indicates the port on which layer-2 protocol tunneling is enabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show registration-table

Function

Run the **show registration-table** command to display the policy of adding the outer VID based on the inner VID of packets.

Syntax

show registration-table [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface of which the policy of adding the outer VID based on the inner VID of packets will be displayed. If this parameter is not specified, the policy of outer VID based on the inner VID of packets on all interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the policy of adding the outer VLAN based on the inner VLAN tag on all the interfaces.

```
Hostname> enable
Hostname# show registration-table
Ports    Type         Outer-VID   Inner-VID-list
------   ----------    ----------  --------------
Gi0/1     Add-outer     10         1-3,5-10
Gi0/1     Add-outer     20         11-20
```

Table 1-7 Output Fields of the show registration-table Command

Field	Description
Ports	Indicates the interface name.
Type	Indicates the type of the protocol-based selective QinQ policy.
Outer-VID	Indicates the added outer VLAN.
Inner-VID-list	Indicates the list of inner VLANs complying with the policy.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show translation-table

Function

Run the **show translation-table** command to display the inner and outer VID modification policy.

Syntax

show translation-table [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface of which the inner VID and outer VID modification policy will be displayed. If this parameter is not specified, the inner VID and outer VID modification policy on all interfaces will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the inner VID and outer VID modification policy.

```
Hostname> enable
Hostname# show translation-table
Ports       Type      Relay-VID  Old-local  Local\inner-VID-list
---------   ---------  ---------  ---------  ---------------------
Gi0/1       Inner-CVID 8         N/A       10-20
Gi0/1       Local-SVID 1001      N/A       30-60
Gi0/1       In+Out     8         20        50
```

Table 1-8 Output Fields of the show translation-table Command

Field	Description
Ports	Indicates the interface name.
Type	Indicates the type of the protocol-based selective QinQ policy.
Relay-VID	Indicates the VLAN ID after the outer/inner tag of input packets is modified.
Old-local	Indicates the VLAN ID of outer tag before modification.
Local\inner-VID-list	Indicates the outer/inner VLAN list before modification.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 switchport dot1q-tunnel allowed vlan

Function

Run the **switchport dot1q-tunnel allowed vlan** command to configure allowed VLANs of the dot1q-tunnel port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The allowed VLAN of dot1q-tunnel port is untagged VLAN 1.

Syntax

switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *svid-list* | [**add**] **untagged** *svid-list* | **remove** *svid-list* }

no switchport dot1q-tunnel allowed vlan

default switchport dot1q-tunnel allowed vlan

Parameter Description

svid-list: VLANs on the SP network. It can contain one or more VLANs. Multiple VLANs are separated by commas. You can also specify a VLAN range by connecting the start VLAN ID and end VLAN ID using an en dash (–).

[**add**] **tagged** *svid-list*: Configures a tagged VLAN allowed by the interface. When output from the interface, packets of this VLAN carry the SP's VLAN tag. No matter whether the **add** parameter is added, the function is consistent.

[**add**] **untagged** *svid-list*: Configures an untagged VLAN allowed by the interface. When output from the interface, packets of this VLAN do not carry the SP's VLAN tag. No matter whether the **add** parameter is added, the function is consistent.

remove *svid-list*: Deletes a VLAN allowed by the interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Run the **show interface dot1q-tunnel** command to display the configuration.

Examples

The following example configures GigabitEthernet 0/1 as dot1q-tunnel port, native VLAN of the interface as VLAN 8. The allowed VLANs of GigabitEthernet 0/1 are untagged VLAN 8 and tagged VLANs 3–6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 8
```

```
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan
untagged 8
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan tagged
3-6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport mode dot1q-tunnel**
- **switchport dot1q-tunnel native vlan**
- **show interfaces dot1q-tunnel**

1.17 switchport dot1q-tunnel native vlan

Function

Run the **switchport dot1q-tunnel native vlan** command to configure the native VLAN of dot1q-tunnel.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the configuration.

The default native VLAN of the dot1q-tunnel port is VLAN 1.

Syntax

switchport dot1q-tunnel native vlan *svid*

no switchport dot1q-tunnel native vlan

default switchport dot1q-tunnel native vlan

Parameter Description

svid: Specifies a VLAN in the SP network as the native VLAN of the dot1q-tunnel port. The value range is from 1 to 4094. Only one native VLAN can be configured.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Run the **show interface dot1q-tunnel** command to display the configuration.

Examples

The following example configures GigabitEthernet 0/1 as dot1q-tunnel port, native VLAN of the interface as VLAN 8. The allowed VLANs of GigabitEthernet 0/1 are untagged VLAN 8 and tagged VLANs 3–6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 8
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan
untagged 8
Hostname(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan tagged
3-6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport mode dot1q-tunnel**
- **switchport dot1q-tunnel allowed vlan**
- **show interfaces dot1q-tunnel**

1.18 switchport mode dot1q-tunnel

Function

Run the **switchport mode dot1q-tunnel** command to configure an interface as a dot1q-tunnel port.

Run **no switchport mode** command to remove this configuration.

Run the **default switchport mode** command to restore the default configuration.

The interface is an access port by default.

Syntax

switchport mode dot1q-tunnel

no switchport mode

default switchport mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

All frames entering the QinQ edge device, regardless of whether they carry IEEE 802.1Q tags, will be encapsulated with one layer of tag. This process is called QinQ encapsulation. The ingress of QinQ edge device is called dot1q-tunnel port, or tunnel port for short. In the basic QinQ, the VLAN ID of an outer tag is the native VLAN of the dot1q-tunnel port. In the selective QinQ, outer tag encapsulation can be implemented according to different encapsulation policies.

Before configuring an encapsulation policy, you need to configure an edge interface as dot1q-tunnel port, and configure native VLAN and allowed VLAN for it.

- If the mode of a layer-2 interface is **dot1q-tunnel**, only one native VLAN is available, and it is VLAN 1 by default. You can use the **switchport dot1q-tunnel native vlan** command to configure the native VLAN as SP VLAN.
- By default, only one allowed VLAN exists and it must be VLAN 1. You can use the **switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlan-list* | [**add**] **untagged** *vlan-list* | **remove** *vlan-list*} command to configure allowed VLANs. The value range is 1 to 4094. The list can contain one or more allowed VLANs. When the packets of all the client VLANs are marked with a unified outer tag, only one allowed VLAN is required; when client VLANs need to be divided into different groups and client packets in different groups are to be marked with different outer tags, multiple allowed VLANs need to be configured.
- The native VLAN must be added to the allowed VLAN list of the interface in an untagged form so that the packets of the SP network can be sent back to the client network after the SP VLAN tags are stripped.
- In the basic QinQ application, the VLANs of the client network do not need to be added to the allowed VLAN list of the tunnel port. In the selective QinQ application, the VLANs of the client network are added to the allowed VLAN list of the interface in the tagged or untagged form.

Run the **show vlan** command to display the configuration.

Examples

The following example configures GigabitEthernet 0/1 as a dot1q-tunnel port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vlan**
- **switchport dot1q-tunnel native vlan**
- **switchport dot1q-tunnel allowed vlan**

1 MSTP Commands

Command	Function
bpdu src-mac-check	Enable the bridge protocol data unit (BPDU) source MAC address check on an interface.
bridge-frame forwarding protocol bpdu	Enable BPDU transparent transmission.
clear spanning-tree counters	Clear statistics on sent and received STP packets.
clear spanning-tree detected-protocols	Clear the original protocol and force the device to migrate to the RSTP protocol.
clear spanning-tree mst topochange record	Clear STP topology change information.
instance	Create/enter an instance and move a VLAN from the original instance to the instance.
l2protocol-tunnel stp	Enable the global STP BPDU tunnel function.
l2protocol-tunnel stp enable	Enable the STP BPDU tunnel function on an interface.
l2protocol-tunnel stp tunnel-dmac	Configure the tunnel address for transmitting STP BPDUs from a customer network.
name	Configure a name for an MST region.
revision	Configure a revision number for an MST region.
show l2protocol-tunnel stp	Display the configuration of a BPDU tunnel.
show spanning-tree	Display the global spanning tree configuration and status information.
show spanning-tree interface	Display the spanning tree configuration and status information of an interface.
show spanning-tree mst	Display the MST region configuration.
show spanning-tree mst topochange record	Display spanning tree topology change records.
spanning-tree	Enable the STP function or configure STP global time parameters.
spanning-tree autoedge	Enable the autoedge function on a designated port.
spanning-tree bpdufilter	Enable the BPDU filter function on an interface so that the interface neither sends nor receives BPDUs, but works in forwarding state.

spanning-tree bpduguard	Enable or disable the BPDU guard function on an interface so that the interface enters error-disabled state when receiving a BPDU.
spanning-tree compatible enable	Enable the spanning tree compatibility mode on an interface.
spanning-tree guard loop	Enable the loop guard function on an interface.
spanning-tree guard none	Disable the guard function on an interface.
spanning-tree guard root	Enable the root guard function on an interface.
spanning-tree ignore tc	Enable the TC filter function on an interface so that the interface diffuses only TC packets generated by itself and does not diffuse received TC packets.
spanning-tree link-type	Forcibly set the connection type of an interface to point-to-point or shared.
spanning-tree loopguard default	Enable the global loop guard function.
spanning-tree mode	Set the spanning tree mode to STP, RSTP, or MSTP.
spanning-tree mst configuration	Enter the MST configuration mode.
spanning-tree mst cost	Configure a port path cost.
spanning-tree mst port-priority	Configure a port priority.
spanning-tree mst priority	Configure a bridge priority.
spanning-tree pathcost method	Configure the method of calculating the default port path cost.
spanning-tree portfast	Configure an interface as an edge port and enable the interface to rapidly enter forwarding state.
spanning-tree portfast bpdufilter default	Enable the global BPDU filter function.
spanning-tree portfast bpduguard default	Enable the global BPDU guard function.
spanning-tree portfast default	Configure all interfaces as edge ports and enable them to rapidly enter forwarding state.
spanning-tree reset	Restore spanning tree parameters to default values.
spanning-tree tc-guard	Enable the TC guard function on an interface.
spanning-tree tc-protection	Enable the global TC protection function.
spanning-tree tc-protection tc-guard	Enable the global TC guard function.

1.1 bpdu src-mac-check

Function

Run the **bpdu src-mac-check** command to enable the bridge protocol data unit (BPDU) source MAC address check on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The BPDU source MAC address check function is disabled on an interface by default.

Syntax

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

default bpdu src-mac-check

Parameter Description

H.H.H: Source MAC address to be matched by BPDUs.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

The Spanning Tree protocol (STP) functions available in interface configuration mode can be configured and take effect only on L2 switching ports. Otherwise, the configuration will fail. If an interface is not an L2 switching port, run the **switchport** command to convert it into an L2 switching port.

If the peer device connects to the local device in a point-to-point manner and the MAC address of the peer device is certain, the BPDU source MAC address check function can be configured on the local device. After this function is enabled, the device receives only BPDU frames matching the designated source MAC address and discards all the other BPDU frames. In addition, when the device encounters BPDU packet attacks, illegitimate BPDU packets can be identified and discarded to prevent the Multiple Spanning Tree Protocol (MSTP) function failure due to the attacks.

Only one BPDU source MAC check address can be configured for one interface.

Examples

The following example enables the BPDU source MAC address check function on port TenGigabitEthernet t 0/1 to receive only BPDU frames whose source MAC address is 00d0.f800.1e2f.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# bpdu src-mac-check 00d0.f800.1e2f
```

Notifications

N/A

Common Errors

An interface is not configured as an L2 switching port, and as a result, the BPDU source MAC address check function fails to be configured.

Platform Description

N/A

Related Commands

N/A

1.2 bridge-frame forwarding protocol bpdu

Function

Run the **bridge-frame forwarding protocol bpdu** command to enable BPDU transparent transmission.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

BPDU transparent transmission is disabled by default.

Syntax

bridge-frame forwarding protocol bpdu

no bridge-frame forwarding protocol bpdu

default bridge-frame forwarding protocol bpdu

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

IEEE 802.1Q uses the destination MAC address (0180.c200.0000) of BPDUs as the reserved address. When a device supporting IEEE 802.1Q receives a frame with the destination address of 0180.c200.0000, it recognizes the frame as a BPDU and will not forward it.

However, in the actual network deployment, some BPDU frames need to be transparently transmitted by devices. For example, STP is disabled on device A but enabled on devices B and C that are connected through device A. In this case, device A needs to transparently transmit BPDU frames so that devices B and C can normally perform STP calculation.

BPDU transparent transmission takes effect only when STP is disabled. When STP is enabled on a device, the device will not transparently transmit BPDU frames.

Examples

The following example enables the BPDU transparent transmission function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bridge-frame forwarding protocol bpdu
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 clear spanning-tree counters

Function

Run the **clear spanning-tree counters** command to clear statistics on sent and received STP packets.

Syntax

clear spanning-tree counters [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Clears statistics on STP packets sent and received by this specified interface.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command is used to clear statistics on sent and received STP packets.

Examples

The following example clears statistics on sent and received STP packets.

```
Hostname> enable
Hostname# clear spanning-tree counters
```

The following example clears statistics on STP packets sent and received by interface TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear spanning-tree counters interface tenGigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp enable**
- **l2protocol-tunnel stp tunnel-dmac**
- **show spanning-tree**

1.4 clear spanning-tree detected-protocols

Function

Run the **clear spanning-tree detected-protocols** command to clear the original protocol and force the device to migrate to the RSTP protocol.

Syntax

clear spanning-tree detected-protocols [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies an interface.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

When finding that the peer device supports the Rapid Spanning Tree Protocol (RSTP), the administrator can configure this command to force all interfaces to send RSTP BPDUs and check the version of received BPDU frames so that the two interconnected devices migrate to RSTP. This function is also called protocol migration.

Examples

The following example clears the original protocol and forces the device to migrate to RSTP.

```
Hostname> enable
Hostname# clear spanning-tree detected-protocols
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 clear spanning-tree mst topochange record

Function

Run the **clear spanning-tree mst topochange record** command to clear STP topology change information.

Syntax

clear spanning-tree mst *instance-id* **topochange record**

Parameter Description

instance-id: Instance ID. The value range is from 0 to 64. Only instance **0** is valid for STP and RSTP.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the spanning tree topology change records, clears the topology change information of STP instance **0**, and then displays the spanning tree topology change records again.

```
Hostname> enable
Hostname# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time             Interface          Old status   New status   Type
2013.5.1 4:18:46   TE0/6              Learning     Forwarding   Normal
Hostname# clear spanning-tree mst 0 topochange record
Hostname# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst topochange record**

1.6 instance

Function

Run the **instance** command to create/enter an instance and move a VLAN from the original instance to the instance.

Run the **no** form of this command to delete an instance (not instance **0**) or move a VLAN in an instance (not instance **0**) to instance **0**.

Run the **default** form of this command to delete an instance (not instance **0**) and move all the VLANs in the instance (not instance **0**) to instance **0**.

Only instance **0** exists and all VLANs belong to instance **0** by default.

Syntax

instance *instance-id* **vlan** *vlan-range*

no instance *instance-id* [**vlan** *vlan-range*]

default instance *instance-id*

Parameter Description

instance-id: Instance ID. The value range is from 0 to 64.

vlan *vlan-range*: Indicates the VLAN list. The value range of a VLAN ID is from 1 to 4094. The VLAN list can contain one or more VLANs. You can separate VLAN IDs by commas (,) or connect continuous VLAN IDs by using a hyphen (-).

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

If a device has a small physical memory (such as 64 MB), creating 64 instances may result in memory insufficiency when devices are stacked. You are advised to control the number of created instances in the case of stacking.

Instance **0** can be neither created nor deleted. Custom instances 1–64 can be created and deleted. You cannot delete VLANs from instance **0** but can delete those from custom instances. Deleting a VLAN from a custom instance will move the VLAN to instance **0**.

In the **instance** *instance-id* **vlan** *vlan-range* command, the value range of *instance-id* is from 0 to 64.

In the **no instance** *instance-id* [**vlan** *vlan-range*] and **default instance** *instance-id* commands, the value of *instance-id* cannot be **0** and its value range is from 1 to 64.

The **no instance** *instance-id* command (without the **vlan** *vlan-range* parameter) command has the same function as the **default instance** *instance-id* command, that is, delete an instance (not instance **0**) and move all the VLANs in the instance (not instance **0**) to instance **0**.

The **no instance** *instance-id* **vlan** *vlan-range* command (carrying the **vlan** *vlan-range* parameter) can move a VLAN in an instance (not instance **0**) to instance **0**. If there are multiple VLANs in the specified instance, you can carry the **vlan** *vlan-range* parameter in this command to move the specified VLANs to instance **0**. Moving all VLANs in an instance to instance **0** will delete the instance.

Examples

The following example enters the MST configuration mode, moves VLAN 3 and VLANs 5–10 to instance **1**, and displays the multiple spanning tree (MST) region configuration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 3, 5-10
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
--------  ----------------
0       1-2,4,11-4094
1       3,5-10
```

The following example moves VLAN 3 from instance **1** to instance **0**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# no instance 1 vlan 3
```

The following example deletes instance **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# no instance 1
```

Notifications

When you move a VLAN to an instance, the following notification will be displayed:

```
%Warning:you must create vlans before configuring instance-vlan relationship.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **name**
- **revision**
- **show spanning-tree mst**

1.7 l2protocol-tunnel stp

Function

Run the **l2protocol-tunnel stp** command to enable the global STP BPDU tunnel function.

Run the **no** form of this command to disable this feature.

The global STP BPDU tunnel function is disabled by default.

Syntax

l2protocol-tunnel stp

no l2protocol-tunnel stp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

In 802.1Q in 802.1Q (QinQ) application, after the STP BPDU tunnel function is enabled, STP packets from the customer network can be transparently transmitted through tunnels of the service provider network. In this way, the STP calculations of the customer network and service provider network are performed separately without mutual interference. 01D0.f800.0005 is the default BPDU tunnel address.

The STP BPDU tunnel function needs to be enabled in both global configuration mode and interface configuration mode so that STP packets can be transparently transmitted through tunnels.

Examples

The following example enables the STP BPDU tunnel function in both global configuration mode and interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# l2protocol-tunnel stp enable
Hostname(config-if-TenGigabitEthernet 0/1)# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
```

```
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp enable**
- **l2protocol-tunnel stp tunnel-dmac**
- **show l2protocol-tunnel stp**

1.8 l2protocol-tunnel stp enable

Function

Run the **l2protocol-tunnel stp enable** command to enable the STP BPDU tunnel function on an interface.

Run the **no** form of this command to disable this feature.

The STP BPDU tunnel function is disabled on an interface by default.

Syntax

l2protocol-tunnel stp enable

no l2protocol-tunnel stp enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In QinQ application, after the STP BPDU tunnel function is enabled, STP packets from the customer network can be transparently transmitted through tunnels of the service provider network. In this way, the STP calculations of the customer network and service provider network are performed separately without mutual interference. 01D0.f800.0005 is the default BPDU tunnel address.

The STP BPDU tunnel function needs to be enabled in both global configuration mode and interface configuration mode so that STP packets can be transparently transmitted through tunnels.

Examples

The following example enables the STP BPDU tunnel function in both global configuration mode and interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-TenGigabitEthernet 0/1)# l2protocol-tunnel stp enable
Hostname(config-if-TenGigabitEthernet 0/1)# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp tunnel-dmac**
- **show l2protocol-tunnel stp**

1.9 l2protocol-tunnel stp tunnel-dmac

Function

Run the **l2protocol-tunnel stp tunnel-dmac** command to configure the tunnel address for transmitting STP BPDUs from a customer network.

Run the **no** form of this command to remove this configuration.

The default tunnel address for transmitting STP BPDUs from a customer network is 01d0.f800.0005.

Syntax

l2protocol-tunnel stp tunnel-dmac *mac-address*

no l2protocol-tunnel stp tunnel-dmac

Parameter Description

mac-address: Tunnel address for transmitting STP BPDUs from a customer network. The value range is 01d0.f800.0005 (default), 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

After an STP packet from a customer network is transmitted to a provider edge (PE) of a service provider network, the PE changes the destination MAC address of the packet from the BPDU dedicated address (0180.c200.0000) to the tunnel address (01d0.f800.0005 by default) and forwards the packet in the service provider network. When the packet reaches a PE at the other end, the PE restores the destination MAC address of the packet from the tunnel address (01d0.f800.0005 by default) to the BPDU dedicated address (0180.c200.0000) and forwards the packet to the peer customer network. The BPDU tunnel function is used to transmit STP packets from a customer network through tunnels in a service provider network so that STP calculations of the customer network and service provider network are performed separately without mutual interference.

Examples

The following example sets the tunnel address for transmitting STP BPDUs from a customer network to 011a.a900.0005.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

Notifications

When the configured tunnel address for transmitting STP BPDUs from a customer network is not within the above range, the following notification will be displayed:

```
Optional at the following addresses: 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003
or 0100.0ccd.cdd0-d2.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp enable**
- **show l2protocol-tunnel stp**

1.10 name

Function

Run the **name** command to configure a name for an MST region.

Run the **no** form of this command to remove this configuration.

The default name of an MST region is an empty string.

Syntax

name *name*

no name

Parameter Description

name: Name of an MST region. The value is a string of up to 32 bytes.

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

The **show spanning-tree mst configuration** command is used to display information about the current MST region, including the name of the MST region.

Examples

The following example enters the MST configuration mode and sets the name of an MST region to Region 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# name region1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **revision**
- **show spanning-tree mst**

1.11 revision

Function

Run the **revision** command to configure a revision number for an MST region.

Run the **no** form of this command to remove this configuration.

The default revision number of an MST region is **0**.

Syntax

revision *version*

no revision

Parameter Description

version: Revision number of an MST region. The value range is from 0 to 65535.

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

The **show spanning-tree mst configuration** command is used to display information about the current MST region, including the revision number of the MST region.

Examples

The following example enters the MST configuration mode and sets the revision number of an MST region to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# revision 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **name**
- **show spanning-tree mst**

1.12 show l2protocol-tunnel stp

Function

Run the **show l2protocol-tunnel stp** command to display the configuration of a BPDU tunnel.

Syntax

show l2protocol-tunnel stp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the configuration of a BPDU tunnel.

```
Hostname> enable
Hostname# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address:011a.a900.0005
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Table 1-1 Output Fields of the show l2protocol-tunnel stp Command

Field	Description
L2protocol-tunnel	Whether the L2 protocol tunnel function is enabled ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
L2protocol-tunnel destination mac address	MAC address of the L2 protocol tunnel
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable	Port with the L2 protocol tunnel function enabled

Notifications

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp enable**
- **l2protocol-tunnel stp tunnel-dmac**

1.13 show spanning-tree

Function

Run the **show spanning-tree** command to display the global spanning tree configuration and status information.

Syntax

show spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **mst** *instance-id* | **pathcost method** | **tx-hold-count**]

show spanning-tree [**counters** | **inconsistentports** | **summary**]

show spanning-tree [**v-stp information**]

Parameter Description

forward-time: Displays the port status change interval (**Bridge Forward Delay**).

hello-time: Displays the interval for periodically sending BPDUs (**Bridge Hello Time**).

max-age: Displays the maximum timeout time of a BPDU (**Bridge Max Age**).

mst *instance-id*: Displays the global spanning tree configuration of a specified instance.

max-hops: Specifies the maximum hop count of BPDUs.

pathcost method: Displays the path cost calculation method.

tx-hold-count: Displays the maximum number of BPDUs that can be sent per second.

counters: Displays statistics on sent and received STP packets.

inconsistentports: Displays ports blocked due to root guard or loop guard.

summary: Displays the spanning tree topology and port forwarding status.

v-stp information: Displays information about the V-STP function.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

Packets with the timeout time out of **max-age** will be discarded.

Forward-time indicates the interval for STP to transition from the listening state to the learning state or from the learning state to the forwarding state. After port role election is complete, a port waits for twice the period of **Forward Delay** before entering the forwarding state.

The restrictive relationship among the values of **forward-time, hello-time, and max-age** is as follows: 2 × (**Hello Time** + 1s) ≤ **Max Age** ≤ 2 × (**Forward Delay** – 1s). The values must meet this condition. Otherwise, the topology may be unstable.

A device selects an interface with the minimum sum of root path costs as the root port. Configuring **pathcost method** (the default value is **long**) will affect the port path cost and further affect the topology of the entire network.

The **show spanning-tree** command displays spanning tree information only after the **spanning-tree** command is run to enable STP.

Examples

The following example displays the global spanning tree configuration. All information will be displayed if no parameter is carried in the command. If parameters [**forward-time** | **hello-time** | **max-age** | **max-hops** | **mst** *instance-id* | **pathcost method** | **tx-hold-count**] are carried, specified global configuration will be displayed.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree
Hostname(config)# show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef  : Disabled

###### mst 0 vlans map : ALL
BridgeAddr : 00d0.f822.4444
Priority: 32768
TimeSinceTopologyChange : 3d:20h:16m:49s
TopologyChanges : 0
DesignatedRoot : 32768.00d0.f822.4444
RootCost : 0
RootPort : 0
CistRegionRoot : 32768.00d0.f822.4444
CistPathCost : 0
```

The following example displays the interval for sending STP BPDUs after the **hello-time** parameter is carried in the command.

```
Hostname> enable
```

```
Hostname# show spanning-tree hello-time
BridgeHelloTime :2
```

The following example displays global spanning tree configuration of instance **0** after the **mst** *instance-id* parameter is carried in the command.

```
Hostname# show spanning-tree mst 0

###### MST 0 vlans mapped : ALL
BridgeAddr : 00d0.f822.4444
Priority: 32768
TimeSinceTopologyChange : 3d:21h:7m:35s
TopologyChanges : 0
DesignatedRoot : 32768.00d0.f822.4444
RootCost : 0
RootPort : 0
CistRegionRoot : 32768.00d0.f822.4444
CistPathCost : 0
```

Table 1-2 Output Fields of the show spanning-tree Command

Field	Description
StpVersion	STP version ● MSTP ● RSTP ● STP
SysStpStatus	STP status ● ENABLED ● DISABLED
Max Age	Aging time of STP BPDUs. The default value is **20**.
Hello Time	Interval for STP to send two adjacent BPDUs. The default value is **2**.
Forward Delay	Duration of STP in the listening and learning states. The default value is **15**.
BridgeMaxAge	Aging time of BPDUs on this device. The default value is **20**.
BridgeHelloTime	Interval for the device to send two adjacent BPDUs. The default value is **2**.
BridgeForwardDelay	Duration of STP in the listening and learning states on this device. The default value is **15**.
MaxHops	Maximum hop count of BPDUs. The default value is **20**.
PathCostMethod	Path cost calculation method ● **long**: Uses the path cost specified in IEEE 802.1t.

Field	Description
	● **long standard**: Calculates the cost value by using a formula according to IEEE 802.1t. ● **short**: Uses the path cost specified in IEEE 802.1d.
TxHoldCount	Maximum number of BPDUs that can be sent per second
BPDUGuard	Status of the global BPDU guard function ● Enabled ● Disabled
BPDUFilter	Status of the global BPDU filter function ● Enabled ● Disabled
LoopGuardDef	Status of the global loop guard function ● Enabled ● Disabled
BridgeAddr	Bridge address of the device
Priority	Bridge priority of the device
TimeSinceTopologyChange	Time that has elapsed since the last topology change, in the format of "d:h:m:s", that is, "day:hour:minute:second".
TopologyChanges	Number of topology change times
DesignatedRoot	ID of a designated bridge
RootCost	Root path cost
RootPort	Root port
CistRegionRoot	Bridge ID of a region root
CistPathCost	Path cost from the region root to CIST root

The following example displays ports that are blocked due to root guard or loop guard.

```
Hostname> enable
Hostname# show spanning-tree inconsistentports
Name               Interface            Inconsistent
-------------------- ---------------------- ------------------

Current Number of Inconsistent ports    :   0
```

Table 1-3 Output Fields of the show spanning-tree Command

Field	Description

Field	Description
Name	Name
Port	Port name
Inconsistent	Blocking status
Current Number of Inconsistent ports	Number of ports that are blocked due to root guard or loop guard

The following example displays statistics on sent and received STP packets.

```
Hostname> enable
Hostname# show spanning-tree counters
---------------------- STP BPDU count ----------------------
 Port                        Receive         Send
 TenGigabitEthernet 0/1             0            122594

------------------------- STP TC or TCN count -------------------------
 MSTID     Port                          Receive     Send
 0         TenGigabitEthernet 0/1            0          0
```

Table 1-4 Output Fields of the show spanning-tree Command

Field	Description
Port	Port ID
Receive	Number of packets received by the port
Send	Number of packets sent by the port
MSTID	Spanning tree instance ID

The following example displays the spanning tree topology and port forwarding status.

```
Hostname> enable
Hostname # show spanning-tree summary
Spanning tree enabled protocol stp
  Root ID    Priority    0
           Address    00d0.f822.3344
           this bridge is root
           Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    0
           Address    00d0.f822.3344
           Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface       Role Sts Cost      Prio    OperEdge Type
```

```
---------------- ---- --- ---------- -------- -------- ----------------
Te0/2            Desg FWD 20000     128      False    P2p
Te0/1            Desg FWD 20000     128      False    P2p
```

Table 1-5 Output Fields of the show spanning-tree Command

Field	Description
Root ID	Spanning tree information of the root device recognized by the local device
Bridge ID	Spanning tree information of the local device
Priority	Bridge priority
Address	Device MAC address
Hello Time	Interval for sending two adjacent BPDUs
Forward Delay	Duration of STP in the listening and learning states
Max Age	Aging time of BPDUs
Port	STP port
Role	Port role
Sts	Port status
Cost	Port path cost
Prio	Port priority
OperEdge	Edge port attribute ● **True**: Edge port ● **False**: Non-edge port
Type	Port connection status ● **P2p**: Point-to-point connection ● **Shared**: Shared connection

The following example displays V-STP information.

```
Hostname> enable
Hostname# show spanning-tree v-stp information
V-STP status              : disable
Local bridge mac           : 00d0.f822.4444
Selected bridge mac        : 0000.0000.0000
Peerlink Port             : Virtual-port
Calculate Virtual Index    : 4095
Mlag Remote device connected : N
MST 0 Root Port        : None
```

Table 1-6 Output Fields of the show spanning-tree Command

Field	Description
V-STP status	V-STP status ● enable ● disable
Local bridge mac	MAC address of the local bridge
Selected bridge mac	MAC address of the selected bridge
Peerlink Port	Peerlink port of an M-LAG group
Calculate Virtual Index	Calculated virtual index
Mlag Remote device connected	Connection status of the M-LAG remote device ● **Y**: Connected ● **N**: Disconnected
MST 0 Root Port	Root port of instance **0**

Notifications

If the global spanning tree configuration is queried when STP is disabled, the following notification will be displayed:

```
No spanning tree instance exists.
```

Platform Description

N/A

Related Commands

- **spanning-tree**
- **spanning-tree pathcost method**

1.14 show spanning-tree interface

Function

Run the **show spanning-tree interface** command to display the spanning tree configuration and status information of an interface.

Syntax

show spanning-tree [**mst** *instance-id*] **interface** *interface-type interface-number* [**bpdufilter** | **bpduguard** | **link-type** | **portfast**]

show spanning-tree [**mst** *instance-id*] *port-index*

Parameter Description

mst *instance-id*: Displays the configuration and status information of an interface in a specified instance.

interface *interface-type interface-number*: Displays the spanning tree configuration and status information of an interface by interface type and interface number (for example, TenGigabitEthernet 0/1).

port-index: Displays the spanning tree configuration and status information of an interface by interface number (for example, 1). The value range is from 0 to 65535. The actual value cannot exceed the maximum port ID. TenGigabitEthernet 0/1 is 1 and *port-index* of port TenGigabitEthernet 0/2 is 2.

bpdufilter: Displays whether the BPDU filter function is enabled on an interface.

bpduguard: Displays whether the BPDU guard is enabled on an interface.

link-type: Displays the connection type of an interface.

portfast: Displays whether the fast forwarding function is enabled on an interface and whether the interface is an edge port.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

For an interface in up state, you can run the **show spanning-tree interface** *interface-type interface-number* command without any parameter to display all characteristic states of the interface. For an interface in down state, the above command cannot display all characteristic states but you can run the [**bpdufilter** | **bpduguard** | **link-type** | **portfast**] command with parameters contained in the command to display required information.

Examples

The following example displays the statuses of interfaces TenGigabitEthernet 0/1 and TenGigabitEthernet 0/2.

```
Hostname> enable
Hostname(config)# show interface description
Interface               Status   Administrative Description
------------------------ -------- -------------- -----------
TenGigabitEthernet 0/1       up      up
TenGigabitEthernet 0/2       down    up
Hostname(config)# exit
```

The following example displays the spanning tree configuration of port TenGigabitEthernet 0/1 (the port status is up).

```
Hostname# show spanning-tree interface tenGigabitEthernet 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
```

```
PortGuardmode  : None

###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
```

The following example displays the spanning tree configuration of port TenGigabitEthernet 0/2 (the port status is down).

```
Hostname# show spanning-tree interface tenGigabitEthernet 0/2
no spanning tree info available for TenGigabitEthernet 0/2.
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 bpdufilter
PortBPDUFilter : Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 portfast
PortAdminPortFast :Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 bpduguard
PortBPDUGuard : Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 link-type
PortAdminLinkType : auto
```

Table 1-7 Output Fields of the show spanning-tree interface Command

Field	Description
PortAdminPortFast	Whether a fast forwarding port is configured
PortOperPortFast	Whether the port is in fast forwarding state
PortAdminAutoEdge	Whether an autoedge port is configured
PortOperAutoEdge	Whether the port is in autoedge state
PortAdminLinkType	Link type configured for the port
PortOperLinkType	Actual link type of the port
PortBPDUGuard	Status of the BPDU guard function of the port
PortBPDUFilter	Status of the BPDU filter function of the port
PortGuardmode	Port guard mode
MST *instance-id* vlans mapped	VLAN list mapped to an instance

Field	Description
PortState	Port forwarding status in an instance
PortPriority	Port priority in an instance
PortDesignatedRoot	Designated root bridge of the port in an instance
PortDesignatedCost	External root path cost of the port in an instance
PortDesignatedBridge	Designated bridge of the port in an instance
PortDesignatedPortPriority	Priority of the designated port in an instance
PortDesignatedPort	Designated port in an instance
PortForwardTransitions	Number of times that the port transitions to the forwarding state in an instance
PortAdminPathCost	Path cost configured for the port in an instance
PortOperPathCost	Actual path cost of the port in an instance
Inconsistent states	Root or loop inconsistent state of the port in an instance
PortRole	Port role

Notifications

When you view all spanning tree information of a port in down state, the following notification will be displayed:

```
no spanning tree info available for TenGigabitEthernet 0/2.
```

When you enter a value in the range of 0 to 65535 but beyond the port ID in the *port-index* parameter, the following notification will be displayed:

```
no spanning tree info available for the interface.
```

Platform Description

N/A

Related Commands

- **spanning-tree autoedge**
- **spanning-tree bpdufilter**
- **spanning-tree bpduguard**
- **spanning-tree link-type**
- **spanning-tree portfast**

1.15 show spanning-tree mst

Function

Run the **show spanning-tree mst** command to display the MST region configuration.

Syntax

show spanning-tree mst configuration

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the MST region configuration before an instance is configured.

```
Hostname> enable
Hostname# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : ALL
-----------------------------------------------------
```

The following example displays the MST region configuration after VLAN 1 is added to instance 1.

```
Hostname> enable
Hostname# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : test
Revision : 0
Instance  Vlans Mapped
--------  ---------------
0       : 2-4094
1       : 1
-------------------------
```

Table 1-8 Output Fields of the show spanning-tree mst Command

Field	Description
Multi spanning tree protocol	Whether MSTP is enabled
Name	Name of an MST region
Revision	Version of the MST region

Field	Description
Instance Vlans Mapped	Mapping between instances and VLANs

Notifications

N/A

Platform Description

N/A

Related Commands

- **instance**
- **name**
- **revision**
- **spanning-tree**
- **spanning-tree mst configuration**
- **spanning-tree mst cost**
- **spanning-tree mst port-priority**
- **spanning-tree mst priority**

1.16 show spanning-tree mst topochange record

Function

Run the **show spanning-tree mst topochange record** command to display spanning tree topology change records.

Syntax

show spanning-tree mst *instance-id* **topochange record**

Parameter Description

instance-id: ID of a specified instance whose spanning tree topology changes need to be displayed. The value range is from 0 to 64. Instance **0** exists by default and instances 1–64 can be customized.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display topology changes of an interface by instance, including the interface experiencing a status change, status change time, old status, new status, and cause for the status change.

Examples

The following example displays the spanning tree topology change records of instance 0.

```
Hostname> enable
Hostname# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time              Interface        Old status   New status    Type
2013.5.1 4:18:46     Te0/1           Learning     Forwarding    Normal
```

Table 1-9 Output Fields of the show spanning-tree mst topochange record Command

Field	Description
Time	Topology change time of an interface
Port	Interface experiencing the topology change
Old status	Old spanning tree status of the interface ● **Discarding**: Discarded state ● **Learning**: Learning state ● **Forwarding**: Forwarding state
New status	New spanning tree status of the interface ● **Discarding**: Discarded state ● **Learning**: Learning state ● **Forwarding**: Forwarding state
Type	Cause for the topology change of the interface. The possible causes are as follows: ● **Normal**: Normal status change of the interface, for example, status change when the interface is up/down. ● **LoopGuard Block**: The interface enters blocking state due to loop inconsistency. ● **RootGuard Block**: The interface enters blocking state due to root inconsistency. ● **Inferior Block**: The interface enters blocking state because it receives a BPDU of a lower priority. ● **LoopGuard Unblock**: The interface recovers from loop inconsistency and enters forwarding state. ● **RootGuard Unblock**: The interface recovers from root inconsistency and enters forwarding state. ● **Inferior Unblock**: The interface does not receive BPDUs of a lower priority and enters forwarding state.

Notifications

When a specified instance does not have topology change, the following notification will be displayed ([dec] indicates the instance ID):

```
%There's no topology change information has been record on mst [ dec ].
```

Platform Description

N/A

Related Commands

- **clear spanning-tree mst topochange record**

1.17 spanning-tree

Function

Run the **spanning-tree** command to enable the STP function or configure STP global time parameters.

Run the **no** form of this command to disable this feature or remove this configuration.

Run the **default** form of this command to restore the default configuration.

The STP function is enabled by default.

The STP function is disabled by default.

Syntax

spanning-tree [**forward-time** *forward* | **hello-time** *hello* | **max-age** *age* | **max-hops** *hop-count* | **timer-factor** *factor* | **tx-hold-count** *count*]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count**]

default spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count** }

spanning-tree [**forward-time** *forward* | **hello-time** *hello* | **max-age** *age* | **max-hops** *hop-count* | **tx-hold-count** *count*]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count**]

default spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count** }

Parameter Description

forward-time *forward*: Specifies the port status change interval, in seconds. After port role election is complete, STP waits for twice the period of **Forward Delay** before entering the forwarding state, that is, the interval for STP to transition from listening state to learning state and from learning state to forwarding state. The value range is from 4 to 30. The default value is **15**.

hello-time *hello*: Specifies the interval for the device to periodically send BPDUs, in seconds. The value range is from 1 to 10. The default value is **2**.

max-age *age*: Specifies the maximum timeout time of BPDUs, in seconds. Packets beyond **max age** will be discarded. The value range is from 6 to 40. The default value is **20**.

max-hops *hop-count*: Specifies the maximum hop count of BPDU frames of all MSTIs, that is, the number of devices that BPDUs of MSTIs can pass through before the BPDUs are discarded. The value range is from 1 to 40, and the default value is **20**.

tx-hold-count *count*: Configures the maximum number of BPDUs that can be sent per second. The value range is from 1 to 10, and the default value is **3**.

timer-factor *factor*: Configures the packet receiving timeout factor. Timeout time = Timeout factor (indicated by *factor*) × Hello Time. If a device fails to receive a BPDU from the upstream device within the timeout time, it re-calculates the spanning tree. The value range is from 1 to 30, and the default value is **20**.

timer-factor *factor*: Configures the packet receiving timeout factor. The timeout time is calculated as follows: Timeout time = Timeout factor (indicated by *factor*) × Hello Time. If a device fails to receive a BPDU from the upstream device within the timeout time, it re-calculates the spanning tree. The value range is from 1 to 30, and the default value is **3**.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The restrictive relationship among the values of **forward-time, hello-time, and max-age** is as follows: 2 × (**Hello Time** + 1s) ≤ **Max Age** ≤ 2 × (**Forward Delay** – 1s). The values must meet this condition. Otherwise, the topology may be unstable.

In an MST region, the BPDU sent by the root bridge contains the **Hot Count** field. The BPDU hop count decreases by 1 each time the BPDU passes through one device from the root bridge till the hop count becomes 0, indicating that the BPDU will be discarded by the receiving device due to timeout. In general, the default value of **max-hops** does not need to be changed for a network with the scale less than 20 hops, but needs to be changed to match the actual network situation when the network scale is greater than 20 hops. Changing the maximum hop count will affect all instances.

You can run the **show spanning-tree** command to display the STP global configuration.

Examples

The following example enables the MSTP function and sets **Forward Delay** to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree
Hostname(config)# spanning-tree forward-time 10
```

The following example sets the maximum number of BPDUs that can be sent per second to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tx-hold-count 5
```

The following example sets the timeout factor to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#spanning-tree timer-factor ?
  <1-30>  Range of timer factor  (default value: 3)
Hostname(config)# spanning-tree timer-factor 4
```

The following example sets the maximum hop count of BPDUs to 30 for all instances on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree max-hops 30
```

Notifications

When the **spanning-tree** command is configured to enable the STP protocol, the following notification will be displayed:

```
Enable spanning-tree.
```

STP and the Transparent Interconnection of Lots of Links (TRILL) protocol of data centers are mutually exclusive. When STP is enabled after TRILL is enabled, the following notification will be displayed:

```
% Error! You must disable TRILL first.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**

1.18 spanning-tree autoedge

Function

Run the **spanning-tree autoedge** command to enable the autoedge function on a designated port.

Run the **spanning-tree autoedge disabled** command to disable this feature.

The autoedge function of a designated port is enabled by default.

Syntax

spanning-tree autoedge [**disabled**]

Parameter Description

disabled: Disables the autoedge function of an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In a spanning tree topology, each LAN connects to the root bridge through a designated port of the upstream node. After this command is configured, if a designated port fails to receive a BPDU from the downstream port within a period of time (3s), it deems that the device connected to this port is a terminal, automatically deems

itself as an edge port, and enters forwarding state. If receiving a BPDU, the port identified as an edge port will be automatically identified as a non-edge port.

Caution

The autoedge function can be enabled only on designated ports.

RSTP and MSTP support the autoedge function but STP does not support the function.

If BPDU filter has been enabled on a port, the port directly enters forwarding state and is not automatically identified as an edge port.

You can run the **show spanning-tree interface** *interface-type interface-number* command to display the spanning tree configuration of an interface. When the value of the **PortAdminAutoEdge** field is **Enabled**, this function is enabled. The value **Disabled** indicates that this function is disabled.

Examples

The following example disables the autoedge function of port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree autoedge disabled
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**

1.19 spanning-tree bpdufilter

Function

Run the **spanning-tree bpdufilter** command to enable the BPDU filter function on an interface so that the interface neither sends nor receives BPDUs, but works in forwarding state.

Run the **spanning-tree bpdufilter disabled** command to disable this feature.

The BPDU filter function is disabled on an interface by default.

Syntax

spanning-tree bpdufilter { **enabled | disabled** }

Parameter Description

enabled: Enables the BPDU filter function on an interface.

disabled: Disables the BPDU filter function on an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

BPDU filter is a method of preventing BPDU attacks. When BPDU filter is enabled, a port neither sends nor receives BPDUs, but directly enters forwarding state. If a port receives a BPDU, it transitions to disabled state and the BPDU filter function automatically fails.

BPDU filter can be enabled globally or on interfaces.

- The **spanning-tree portfast bpdufilter default** command is used to enable the global BPDU filter function. The global BPDU filter function takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with the port fast configuration, the port fast configuration prevails.
- The **spanning-tree bpdufilter enabled** command is used to enable the BPDU filter function on an interface. The function takes effect on the interface regardless of whether the interface is an edge port.

Note

In general, when a port running STP transitions from listening state to learning state and then to forwarding state, it needs to wait for twice the period of **Forward-Delay** (2 × 15 = 30s by default). If a device port directly connects to a network terminal, you can enable the BPDU filter function to enable the port to work in forwarding state.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpdufilter** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the BPDU filter function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree bpdufilter enabled
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**
- **spanning-tree portfast bpdufilter default**

1.20 spanning-tree bpduguard

Function

Run the **spanning-tree bpduguard** command to enable or disable the BPDU guard function on an interface so that the interface enters error-disabled state when receiving a BPDU.

The BPDU guard function is disabled on an interface by default.

Syntax

spanning-tree bpduguard { **enable** | **disabled** }

Parameter Description

enable: Enables the BPDU guard function on an interface.

disabled: Disables the BPDU guard function on an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

If a user illegally connects to a network device to an interface, to which a terminal should be connected, the network device may send BPDUs, causing a network topology change. If an interface with BPDU guard enabled receives a BPDU, it starts the BPDU guard mechanism, enters the error-disabled state, and is disabled, indicating that a network exception occurs.

An interface in error-disabled state can be restored automatically or manually. The **errdisable recovery** [**interval** *seconds*] command is used to configure the interval for automatically restoring a port from error-disabled state, in seconds. The value range is from 30 to 86400. The **errdisable recovery** command is used to manually restore a port from error-disabled state.

BPDU guard can be enabled globally or on interfaces.

- The **spanning-tree portfast bpduguard default** command is used to enable global BPDU guard, which takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with port fast configuration, the port fast configuration prevails.

- The **spanning-tree bpduguard enable** command is used to enable BPDU guard, which takes effect on interfaces regardless of whether they are edge ports.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpduguard** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the BPDU guard function on port TenGigabitEthernet 0/1 and sets the auto-recovery time to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree bpduguard enable
Hostname(config-if-TenGigabitEthernet 0/1)# errdisable recovery interval 60
```

Notifications

When an interface with BPDU guard enabled receives a BPDU, the following notification will be displayed ([char] indicates the interface name):

```
SPANTREE-BLOCK_BPDUGUARD: Received BPDU on port [ char ] with BPDU Guard enabled.
Disabling port.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **errdisable recovery** (interface/Ethernet interface)
- **show spanning-tree interface**
- **spanning-tree portfast bpduguard default**

1.21 spanning-tree compatible enable

Function

Run the **spanning-tree compatible enable** command to enable the spanning tree compatibility mode on an interface.

Run the **no** form of this command to disable this feature.

The spanning tree compatibility mode is enabled on an interface by default.

The spanning tree compatibility mode is disabled on an interface by default.

Syntax

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

After the spanning tree compatibility mode is enabled on an interface, STP calculates whether the interface participates in the calculation of a specified instance based on the VLAN, to which the interface belongs, and the mapping between the VLAN and the instance. When the interface sends a BPDU, only the MSTI configuration message of the instance calculated by the interface, is carried to ensure compatibility with other devices.

For example, instances 1 and 2 exist on a device. Port GigabitEthernet 0/1 belongs only to VLAN 10, and VLAN 10 belongs to instance 1. If the spanning tree compatibility mode is enabled on port GigabitEthernet 0/1, the BPDU sent by port GigabitEthernet 0/1 carries only information of instance 0 (the port participates in calculation of this instance by default) and instance 1, with no information of instance 2.

Examples

The following example creates instance 1 and instance 2, associates instance 1 with VLAN 10 and instance 2 with VLAN 20, adds port TenGigabitEthernet 0/1 to VLAN 10, enables the spanning tree compatibility mode on port TenGigabitEthernet 0/1, and adds port TenGigabitEthernet 0/2 to VLAN 20. After configuration, BPDUs sent by port TenGigabitEthernet 0/1 will not carry information about instance 2 and port TenGigabitEthernet 0/2 will not participate in the spanning tree calculation of instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 10
Hostname(config-mst)# instance 2 vlan 20
Hostname(config-mst)# exit
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode access
Hostname(config-if-TenGigabitEthernet 0/1)# switchport access vlan 10
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree compatible enable
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface Gigabitethernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport
Hostname(config-if-GTenGigabitEthernet 0/2)# switchport mode access
Hostname(config-if-TenGigabitEthernet 0/2)# switchport access vlan 20
Hostname(config-if-TenGigabitEthernet 0/2)# spanning-tree compatible enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree mst configuration**

1.22 spanning-tree guard loop

Function

Run the **spanning-tree guard loop** command to enable the loop guard function on an interface.

Run the **no** function to disable this feature.

The loop guard function is disabled on an interface by default.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

The root port or backup port of a non-root bridge may fail to receive BPDUs due to the unidirectional link failure, and the root port becomes a designated port and enters forwarding state. As a result, loops occur in the network. To prevent this situation, you can configure loop guard on a non-root bridge.

After loop guard is enabled, when the root port or backup port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives a BPDU for spanning tree calculation.

Loop guard can be enabled globally or on interfaces.

- The **spanning-tree loopguard default** command is used to globally enable the loop guard function on all interfaces.
- The **spanning-tree guard loop** command is used to enable the loop guard function on an interface.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the loop guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-GTenGigabitEthernet 0/1)# spanning-tree guard loop
```

Notifications

When loop guard is configured after root guard is configured, the following notification will be displayed ([chars] indicates the interface name):

```
SPANTREE-ROOTGUARD_CONFIG_CHANGE: Root Guard disabled on port [ chars ].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree loopguard default**

1.23 spanning-tree guard none

Function

Run the **spanning-tree guard none** command to disable the guard function on an interface.

Run the **no** form of this command to remove this configuration.

There is no interference in the guard function of an interface by default.

Syntax

spanning-tree guard none

no spanning-tree guard none

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

When an interface is blocked due to root guard, you can manually restore the port to the normal state by using two methods:

- Run the **no spanning-tree guard root** command to disable the root guard function on the interface.
- Run the **spanning-tree guard none** command to disable the guard function on the interface.

Examples

The following example disables the guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree guard none
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree guard root**

1.24 spanning-tree guard root

Function

Run the **spanning-tree guard root** command to enable the root guard function on an interface.

Run the **no** form of this command to disable the root guard function on an interface.

The root guard function is disabled on an interface by default.

Syntax

spanning-tree guard root

no spanning-tree guard root

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the network design, the root bridge and backup root bridge are usually classified into the same region. Designated ports on a root bridge may receive configuration BPDUs with a higher priority due to a

misconfiguration or malicious attacks, and the root bridge loses the current root bridge role. As a result, an incorrect network topology change is incurred. To prevent this situation, you can configure the root guard function on designated ports of the root bridge.

After the root guard function is enabled, the device ports are designated ports on all instances. If a port receives a high-priority BPDU, the port enters blocking state due to root-inconsistent. If the port fails to receive a high-priority BPDU within a period of time, it returns to the normal state.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the root guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree guard root
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree guard loop**
- **spanning-tree guard none**

1.25 spanning-tree ignore tc

Function

Run the **spanning-tree ignore tc** command to enable the TC filter function on an interface so that the interface diffuses only TC packets generated by itself and does not diffuse received TC packets.

Run the **no** function to disable this feature.

The TC filter function is disabled on an interface by default.

Syntax

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.
- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the TC filter function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree ignore tc
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree tc-guard**
- **spanning-tree tc-protection**
- **spanning-tree tc-protection tc-guard**

1.26 spanning-tree link-type

Function

Run the **spanning-tree link-type** command to forcibly set the connection type of an interface to point-to-point or shared.

Run the **no** form of this command to restore the default configuration.

The default connection type of an interface is auto mode. If an interface works in full-duplex mode, the connection type is point-to-point. If an interface works in half-duplex mode, the connection type is shared.

Syntax

spanning-tree link-type { **point-to-point** | **shared** }

no spanning-tree link-type

Parameter Description

point-to-point: Forcibly sets the connection type of an interface to point-to-point.

shared: Forcibly sets the connection type of an interface to shared.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

A designated port of RSTP can perform a Proposal/Agreement handshake with the connected bridge and rapidly enter forwarding state, to implement fast convergence. In this way, the port does not need to wait for twice the period of **Forward Delay** before entering forwarding state. Only interfaces using the point-to-point connection support fast convergence via handshake. You are advised to configure the point-to-point connection for devices, so as to give full play to the devices. If the connection type is not configured, the device automatically sets the port connection type based on the port duplex status.

You can run the **show spanning-tree interface** *interface-type interface-number* **link-type** command to display the spanning tree configuration of an interface. When the **PortAdminLinkType** field is set to **Auto**, the connection type of an interface is auto mode. The value **point-to-point** indicates that the connection type of an interface is forcibly set to point-to-point, and **shared** indicates that the connection type of an interface is forcibly set to non-point-to-point.

Examples

The following example forcibly sets the connection type of port TenGigabitEthernet 0/1 to point-to-point.

```
Hostname> enable
Hostname# show spanning-tree interface gtenGigabitEthernet 0/1 link-type
PortAdminLinkType : auto
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree link-type point-to-point
Hostname(config-if-TenGigabitEthernet 0/1)# end
Hostname# show spanning-tree interface tenGigabitEthernet 0/1 link-type
PortAdminLinkType : point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**

1.27 spanning-tree loopguard default

Function

Run the **spanning-tree loopguard default** command to enable the global loop guard function.

Run the **no** form of this command to restore the default configuration.

The global loop guard function is disabled by default.

Syntax

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The root port or backup port of a non-root bridge may fail to receive BPDUs due to the unidirectional link failure, and the root port becomes a designated port and enters forwarding state. As a result, loops occur in the network. To prevent this situation, you can configure loop guard on a non-root bridge.

After loop guard is enabled, when the root port or backup port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives a BPDU for spanning tree calculation.

Loop guard can be enabled globally or on interfaces.

- The **spanning-tree loopguard default** command is used to globally enable the loop guard function on all interfaces.
- The **spanning-tree guard loop** command is used to enable the loop guard function on an interface.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the global loop guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree loopguard default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree guard loop**

1.28 spanning-tree mode

Function

Run the **spanning-tree mode** command to set the spanning tree mode to STP, RSTP, or MSTP.

Run the **no** form of this command to restore the default configuration.

The default spanning tree mode is MSTP.

Syntax

spanning-tree mode { **mstp** | **rstp** | **stp** }

no spanning-tree mode

Parameter Description

mstp: Indicates the Multiple Spanning Tree Protocol (IEEE 802.1s).

rstp: Indicates the Rapid Spanning Tree Protocol (IEEE 802.1w).

stp: Indicates the Spanning Tree Protocol (IEEE 802.1d).

Command Modes

Global configuration mode

Usage Guidelines

However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the spanning tree mode to a lower version to ensure compatibility.

Caution

- When you switch from the MSTP mode to RSTP or STP mode, all information about MST regions will be cleared.
- The spanning tree mode switching will cause the spanning tree recalculation.

You can run the **show spanning-tree** command to display the spanning tree configuration.

Default Level

15

Examples

The following example switches the spanning tree mode to STP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mode stp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**

1.29 spanning-tree mst configuration

Function

Run the **spanning-tree mst configuration** command to enter the MST configuration mode.

Run the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to enable the MSTP protocol. Devices that have the same configuration name, revision number, and instance mappings constitute an MST region. Configuration names, revision numbers, and instance mappings are recorded in the **MST CFG ID** field of MST BPDUs and they can be configured.

- Configuration name: Identifies an MST region. The value is a string of up to 32 characters and the default value is empty.
- Revision number: Identifies an MST region. The value is a 2-byte non-negative integer and the default value is **0**.
- Instance mapping: Indicates mappings between instances and VLANs. One MST region can contain multiple MSTIs. Instance **0** exists by default and instances 1–64 can be created. This device supports VLANs 1–4094. VLANs belong to instance **0** except those that have been assigned to instances.

MST regions are independent of each other. If a port on a device receives a BPDU with **MST CFG ID** same as that of the MST BPDU of the device, the device deems that the peer device and the device belong to the same MST region. Otherwise, the device deems that the peer device belongs to a different MST region. The load sharing advantage of MSTP can be reflected only after multiple devices are configured to the same MST region. Therefore, MST regions need to be properly divided and devices in the same MST region need to have the same **MST CFG ID**.

Examples

The following example enters the MST configuration mode, configures an MST region named region1, configures instance 1 to include VLAN 3 and VLANs 5–10, and displays the MST region configuration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 3, 5-10
Hostname(config-mst)# name region1
Hostname(config-mst)# revision 1
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 1
```

```
Instance  Vlans Mapped
--------  ---------------
0       1-2,4,11-4094
1       3,5-10
----------------------------
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **name**
- **revision**
- **show spanning-tree mst**

1.30 spanning-tree mst cost

Function

Run the **spanning-tree mst cost** command to configure a port path cost.

Run the **no** command to restore the default configuration.

A device automatically calculates the port path cost based on the link rate of an interface by default.

Syntax

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] **cost**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the port path cost can be configured based on this instance. The value range is from 0 to 64, and the default value is **0**.

cost *cost*: Specifies the port path cost. The value range is from 1 to 200000000. The port path cost is automatically calculated based on the link rate of an interface in accordance with IEEE 802.1t Long by default. For example, as shown in Table 1-10, the path cost of an interface with the rate of 1000 Mbps is 20,000, the path cost of an interface with the rate of 100 Mbps is 200,000, and the path cost of an interface with the rate of 10 Mbps is 2,000,000.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

The root path cost is the sum of path costs of all ports in the path from a device to the root. When the administrator needs to control the spanning tree topology, the port path cost can be modified to affect the root path cost value.

You can run the **show spanning-tree mst interface** *interface-type interface-number* command to verify the above configuration.

Examples

The following example sets the port path cost of port TenGigabitEthernet 0/1 to 400 in instance 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree mst 3 cost 400
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.31 spanning-tree mst port-priority

Function

Run the **spanning-tree mst port-priority** command to configure a port priority.

Run the **no** form of this command to restore the default configuration.

The default port priority is 128.

Syntax

spanning-tree [**mst** *instance-id*] **port-priority** *port-priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the instance-based port priority can be configured. The value range is from 0 to 64, and the default value is **0**.

port-priority *port-priority*: Specifies the port priority. The value range is multiples of 16, that is, 0, 16, 32, 48, 64, 80, 96, 112, 128 (default value), 144, 160, 176, 192, 208, 224, and 240, totaling 16 integers.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

A port ID consists of two bytes, with the first byte of *port-priority* and the second byte of port ID.

When the administrator needs to control the spanning tree topology, he can configure *port-priority* to change the port ID.

You can run the **show spanning-tree mst interface** *interface-type interface-number* command to verify the above configuration.

Examples

The following example sets the port priority of port TenGigabitEthernet 0/1 in instance 20 to 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree mst 20 port-priority 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.32 spanning-tree mst priority

Function

Run the **spanning-tree mst priority** command to configure a bridge priority.

Run the **no** command to restore the default configuration.

The default bridge priority is **32768**.

Syntax

spanning-tree [**mst** *instance-id*] **priority** *priority*

no spanning-tree [**mst** *instance-id*] **priority**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the bridge priority can be configured based on this instance. The value range is from 0 to 64, and the default value is **0**.

priority *priority*: Specifies the bridge priority. The value range is multiples of 4096, that is, 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768 (default value), 36864, 40960, 45056, 49152, 53248, 57344, and 61440, totaling 16 integers.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

A bridge ID consists of eight bytes, with the first two bytes of the bridge priority (indicated by *priority*) and the last six bytes used for the MAC address of the bridge.

When the administrator needs to control the spanning tree topology, *priority* can be changed to change the bridge ID.

After running the **spanning-tree** command to enable STP, you can run the **show spanning-tree** and **show spanning-tree summary** commands to verify the above configuration.

Examples

The following example sets the bridge priority of instance 20 to 8192 in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst 20 priority 8192
```

Notifications

When the configured bridge priority is not a multiple of 4096, the following notification will be displayed:

```
bridge priority must be IN increments of 4096
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.33 spanning-tree pathcost method

Function

Run the **spanning-tree pathcost method** command to configure the method of calculating the default port path cost.

Run the **no** form of this command to restore the default configuration.

The port path cost is calculated according to IEEE 802.1t Long by default.

Syntax

spanning-tree pathcost method { **long** | **long standard** | **short** }

no spanning-tree pathcost method

Parameter Description

long: Sets and calculates the port path cost according to IEEE 802.1t Long.

long standard: Sets and calculates the port path cost according to IEEE 802.1t Long Standard.

short: Sets and calculates the port path cost according to IEEE 802.1d Short.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The methods of calculating the default port path costs specified in standards are listed in Table 1-10. Be sure to adopt a consistent port path cost standard for the entire network.

IEEE 802.1d Short: The range of the port path cost is from 1 to 65535. Aggregate port cost = Physical port cost × 95%.

IEEE 802.1t Long: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost × 95%.

IEEE 802.1t Long Standard: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost/Linkupcnt. At this moment, the cost value of the aggregate port will change with the number of member ports, which will lead to the network topology change. For configurations of aggregate ports and the Link Aggregation Control Protocol (LACP), see *Link Aggregation Port*.

- When an aggregate port is a static aggregate port, **Linkupcnt** refers to the number of member ports in Link Up state.
- When an aggregate port is an LACP aggregate port, **Linkupcnt** refers to the number of member ports participating in the aggregate port data forwarding.
- When no member port of an aggregate port is in Link Up state or forwarding data, the value of **Linkupcnt** is **1**.

Table 1-10 Port Path Costs Calculated Based on the Link Rate

Port Rate	Port	IEEE 802.1d Short	IEEE 802.1t Long	IEEE 802.1t Long Standard
10 Mbps	Common port	100	2000000	2000000
	Aggregate port	95	1900000	2000000/Linkupcnt
100 Mbps	Common port	19	200000	200000
	Aggregate port	18	190000	200000/Linkupcnt
1000 Mbps	Common port	4	20000	20000
	Aggregate port	3	19000	20000/Linkupcnt
10000 Mbps	Common port	2	2000	2000
	Aggregate port	1	1900	20000/Linkupcnt

You can run the **show spanning-tree pathcost method** command to display the configuration.

Examples

The following example sets the port path cost calculation method to **Long Standard**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree pathcost method long standard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**

1.34 spanning-tree portfast

Function

Run the **spanning-tree portfast** command to configure an interface as an edge port and enable the interface to rapidly enter forwarding state.

Run the **spanning-tree portfast disabled** command to remove this configuration.

Interfaces are non-edge ports by default.

Syntax

spanning-tree portfast

spanning-tree portfast disabled

Parameter Description

disabled: Restores an interface to a non-edge port and disables the fast forwarding function of the interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

If you are sure that a device interface is directly connected to a network terminal, you can manually configure the interface as an edge port. An edge port can enter forwarding state rapidly without waiting for twice the period of **Forward Delay**. The global BPDU guard and BPDU filter functions take effect only on edge ports.

- The **spanning-tree portfast default** command is used to configure the port fast attribute for all interfaces.
- The **spanning-tree portfast** command is used to configure the port fast attribute for a specific interface.

You can run the **show spanning-tree interface** *interface-type interface-number* **portfast** command to display the spanning tree configuration of an interface. If the value of the **PortAdminPortFast** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example configures port TenGigabitEthernet 0/1 as an edge port and enables the port to rapidly enter forwarding state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
```

```
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
```

Notifications

When an interface is manually configured as an edge port, the following notification will be displayed:

```
%Warning: portfast should only be enabled on ports connected to a single host. Connecting
hubs, switches, bridges to this interface when portfast is enabled,can cause temporary
loops.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**
- **spanning-tree portfast default**

1.35 spanning-tree portfast bpdufilter default

Function

Run the **spanning-tree portfast bpdufilter default** command to enable the global BPDU filter function.

Run the **no** form of this command to disable the global BPDU filter function.

The global BPDU filter function is disabled by default.

Syntax

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

BPDU filter is a method of preventing BPDU attacks. When BPDU filter is enabled, a port neither sends nor receives BPDUs, but directly enters forwarding state. If a port receives a BPDU, it transitions to disabled state and the BPDU filter function automatically fails.

BPDU filter can be enabled globally or on interfaces.

- The **spanning-tree portfast bpdufilter default** command is used to enable the global BPDU filter function. The global BPDU filter function takes effect only on edge ports. Edge ports can be automatically identified by

the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with the port fast configuration, the port fast configuration prevails.

- The **spanning-tree bpdufilter enabled** command is used to enable the BPDU filter function on an interface. The function takes effect on the interface regardless of whether the interface is an edge port.

Note

In general, when a port running STP transitions from listening state to learning state and then to forwarding state, it needs to wait for twice the period of **Forward-Delay** (2 × 15 = 30s by default). If a device port directly connects to a network terminal, you can enable the BPDU filter function to enable the port to work in forwarding state.

You can run the **show spanning-tree** command to display the configuration.

Examples

The following example enables the global BPDU filter function and configures port TenGigabitEthernet 0/1 as an edge port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree portfast bpdufilter default
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**
- **spanning-tree bpdufilter**
- **spanning-tree portfast**

1.36 spanning-tree portfast bpduguard default

Function

Run the **spanning-tree portfast bpduguard default** command to enable the global BPDU guard function.

Run the **no** form of this command to disable this feature.

The global BPDU guard function is disabled by default.

Syntax

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If a user illegally connects to a network device to an interface, to which a terminal should be connected, the network device may send BPDUs, causing a network topology change. If an interface with BPDU guard enabled receives a BPDU, it starts the BPDU guard mechanism, enters error-disabled state, and is disabled, indicating that an error occurs. An interface in error-disabled state can be restored automatically or manually. You can run the **errdisable recovery** [**interval** *seconds*] command to configure the interval for automatically restoring a port, in seconds. The value range is from 30 to 86400. If the command carries no parameter, the port needs to be manually restored.

BPDU guard can be enabled globally or on interfaces.

- The **spanning-tree portfast bpduguard default** command is used to enable global BPDU guard, which takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with port fast configuration, the port fast configuration prevails.
- The **spanning-tree bpduguard enabled** command is used to enable BPDU guard, which takes effect on interfaces regardless of whether they are edge ports.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpduguard** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the global BPDU guard function, configures port TenGigabitEthernet 0/1 as an edge port, and sets the auto-recovery time to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree portfast bpduguard default
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
Hostname(config-if-TenGigabitEthernet 0/1)# errdisable recovery interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**
- **spanning-tree bpduguard**
- **spanning-tree portfast**

1.37 spanning-tree portfast default

Function

Run the **spanning-tree portfast default** command to configure all interfaces as edge ports and enable them to rapidly enter forwarding state.

Run the **no** form of this command to remove this configuration.

All interfaces are non-edge ports by default.

Syntax

spanning-tree portfast default

no spanning-tree portfast default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If you are sure that a device interface is directly connected to a network terminal, you can manually configure the interface as an edge port. An edge port can enter forwarding state rapidly without waiting for twice the period of **Forward Delay**. The global BPDU guard and BPDU filter functions take effect only on edge ports.

- The **spanning-tree portfast default** command is used to configure the port fast attribute for all interfaces.
- The **spanning-tree portfast** command is used to configure the port fast attribute for a specific interface.

You can run the **show spanning-tree interface** *interface-type interface-number* **portfast** command to display the spanning tree configuration of an interface. If the value of the **PortAdminPortFast** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example configures all interfaces as edge ports and enables them to rapidly enter forwarding state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree portfast default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree portfast**

1.38 spanning-tree reset

Function

Run the **spanning-tree reset** command to restore spanning tree parameters to default values.

Syntax

spanning-tree reset

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command does not have the **no** form.

When STP is enabled, configuring the **spanning-tree reset** command cannot restore STP to the default disabled state.

Examples

The following example restores all spanning tree parameters to default values.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# spanning-tree reset
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 spanning-tree tc-guard

Function

Run the **spanning-tree tc-guard** command to enable the TC guard function on an interface.

Run the **no** form of this command to disable this feature.

The TC guard function is disabled on an interface by default.

Syntax

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period

expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.

- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the TC guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree tc-guard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree ignore tc**
- **spanning-tree tc-protection**
- **spanning-tree tc-protection tc-guard**

1.40 spanning-tree tc-protection

Function

Run the **spanning-tree tc-protection** command to enable the global TC protection function.

Run the **no** form of this command to disable this feature.

TC protection is disabled by default.

Syntax

spanning-tree tc-protection

no spanning-tree tc-protection

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.
- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the global TC protection function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tc-protection
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree ignore tc**
- **spanning-tree tc-guard**
- **spanning-tree tc-protection tc-guard**

1.41 spanning-tree tc-protection tc-guard

Function

Run the **spanning-tree tc-protection tc-guard** command to enable the global TC guard function.

Run the **no** form of this command to disable this feature.

The global TC guard function is disabled by default.

Syntax

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If

the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.

- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the global TC guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tc-protection tc-guard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree ignore tc**
- **spanning-tree tc-guard**
- **spanning-tree tc-protection**

1 ERPS Commands

Command	Function
associate sub-ring raps-vlan	Associate major rings of Ethernet intersecting rings with subrings.
erps enable	Enable the global ERPS function.
erps monitor link-state by oam	Monitor the logical status of ERPS links through OAM.
erps raps-vlan	Create an Ethernet ring R-APS VLAN and enter the R-APS VLAN configuration mode.
protected-instance	Configure the VLANs protected by an Ethernet ring.
ring-port	Add ports to an ERPS ring.
rpl-port	Configure the RPL port for an ERPS ring.
show erps	Display the parameters and state of ERPS.
state enable	Enable the ERPS function for a specified ring.
sub-ring tc-propagation	Enable the subring topology change notification.
timer	Configure ERPS timers.

1.1 associate sub-ring raps-vlan

Function

Run the **associate sub-ring raps-vlan** command to associate major rings of Ethernet intersecting rings with subrings.

Run the **no** form of this command to remove this configuration.

A major ring of Ethernet intersecting rings is not associated with its subrings by default.

Syntax

associate sub-ring raps-vlan *vlan-list*

no associate sub-ring raps-vlan *vlan-list*

Parameter Description

vlan-list: R-APS VLAN list of subrings. The value range is from 1 to 4094. The VLAN list can contain one or more VLANs. When multiple VLANs are contained, separate VLAN IDs by a comma (,) or connect continuous VLAN IDs with a hyphen (-).

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

This command needs to be configured on all nodes in an Ethernet Ring Protection Switching (ERPS) major ring so that ERPS packets of its subrings can be transmitted in the major ring.

The association aims to ensure that ERPS packets of the subrings can be transmitted in other Ethernet rings. You can also use the command provided by the VLAN module to configure a VLAN and its member ports so that ERPS packets of subrings can be transmitted in the major ring and are not leaked to user networks.

Examples

The following example associates the major ring R-APS VLAN 4093 with the subring R-APS VLAN 100 in an Ethernet.

(1) The following example configures the links of ports (TenGigabitEthernet 0/1 and TenGigabitEthernet 0/2) in the major ring to work in trunk mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface tenGigabitEthernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/2)# exit
```

(2) The following example configures R-APS VLAN 4093, adds the ports to the Ethernet ring, specifies the ring protection link (RPL) port and RPL owner, and enables the ERPS function.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps 4093)# ring-port west tenGigabitEthernet 0/1 east
tenGigabitEthernet 0/2
Hostname(config-erps 4093)# rpl-port east rpl-owner
Hostname(config-erps 4093)# state enable
Hostname(config-erps 4093)# exit
```

(3) The following example enables the ERPS function globally.

```
Hostname(config)# erps enable
```

(4) The following example configures the link mode for the subring port, configures R-APS VLAN 100, adds TenGigabitEthernet 0/3 to the Ethernet ring, and enables the ERPS function.

```
Hostname(config)# erps raps-vlan 100
Hostname(config)# interface tenGigabitEthernet 0/3
Hostname(config-if-TenGigabitEthernet 0/3)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/3)# exit
Hostname(config)# erps raps-vlan 100
Hostname(config-erps 100)# ring-port west tenGigabitEthernet 0/3 east
virtual-channel
Hostname(config-erps 100)# state enable
Hostname(config-erps 100)# exit
```

(5) The following example associates the major ring R-APS VLAN 4093 with the subring R-APS VLAN 100.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps4093)# associate sub-ring raps-vlan 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps enable**
- **erps raps-vlan**
- **ring-port**
- **state enable**

1.2 erps enable

Function

Run the **erps enable** command to enable the global ERPS function.

Run the **no** form of this command to disable this feature.

The global ERPS function is disabled by default.

Syntax

erps enable

no erps enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

ERPS, also known as G.8032, is a ring protection protocol specially designed for the link layer in an Ethernet ring. It eliminates loops in the link layer in an Ethernet ring and prevents broadcast storms caused by data loops by blocking the specified ports. ERPS can rapidly recover the communication between nodes in the event that a link is disconnected in the Ethernet ring. ERPS has the L2 convergence time less than 50 ms, while the L2 convergence time is 50s for the Spanning Tree Protocol (STP) with similar functions, and nearly 1s for the Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

ERPS takes effect in a specified ring only after ERPS is enabled globally and for the ring.

Run the **state enable** command to enable the ERPS function for a specified ring.

Examples

The following example enables the ERPS function globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# erps enable
```

The following example enables the ERPS function for a specified ring in R-APS VLAN configuration mode.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps4093)# state enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **state enable**

1.3 erps monitor link-state by oam

Function

Run the **erps monitor link-state by oam** command to monitor the logical status of ERPS links through OAM.

Run the **no** form of this command to directly monitor the physical status of ERPS links.

The physical status of ERPS links is directly monitored by default.

Syntax

erps monitor link-state by oam vlan *vlan-id*

no erps monitor link-state by oam

Parameter Description

vlan-id: ID of the VLAN that uses OAM to monitor the link status. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

There are two methods of monitoring the ERPS link status.

- The physical status of ERPS links is directly monitored: up or down. This method is highly efficient.
- The logic status of ERPS links is monitored through OAM: unidirectional failure, bidirectional failure, or normal. This method is less efficient and the convergence time may be longer when the topology changes.

Examples

The following example monitors the logical status of ERPS links through OAM.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# erps monitor link-state by oam vlan 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps enable**

1.4 erps raps-vlan

Function

Run the **erps raps-vlan** command to create an Ethernet ring R-APS VLAN and enter the R-APS VLAN configuration mode.

Run the **no** form of this command to remove this configuration.

No R-APS VLAN is configured by default.

Syntax

erps raps-vlan *vlan-id*

no erps raps-vlan *vlan-id*

Parameter Description

vlan-id: ID of an R-APS VLAN. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An R-APS VLAN must be an unused VLAN on a device. VLAN 1 cannot be configured as an R-APS VLAN.

In an Ethernet ring, different devices must be configured with the same R-APS VLAN.

If a device with ERPS disabled needs to transparently transmit ERPS packets, ensure that only the two ports connecting the device to an ERPS ring allow packets from the ERPS ring to pass. Otherwise, packets from other VLANs may be transparently transmitted to the R-APS VLAN, causing impact on the ERPS ring.

Examples

The following example configures the R-APS VLAN 4093 for an Ethernet ring.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps4093)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps enable**

1.5 protected-instance

Function

Run the **protected-instance** command to configure the VLANs protected by an Ethernet ring.

Run the **no** form of this command to configure an Ethernet ring to protect all VLANs.

An Ethernet ring protects all VLANs by default.

Syntax

protected-instance *instance-id-list*

no protected-instance

Parameter Description

instance-id-list: List of the instances protected by an Ethernet ring. The VLAN group corresponding to an instance needs to be configured to configure the protected VLANs for an Ethernet ring. The value range is from 0 to 64. The instance list can contain one or more instances. When multiple instances are configured, separate the instances by a comma (,) and separate continuous instances with a hyphen (-).

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

Instances protected by an Ethernet ring can implement load balancing.

Examples

The following example configures ERPS 1 and ERPS 2 on a device to implement load balancing. In ERPS 1, the R-APS VLAN is VLAN 100, and protected data VLANs are 1-99 and 101-2000. In ERPS 2, the R-APS VLAN is VLAN 4093, and protected data VLANs are 2001-4092 and 4094. The load balancing is configured as follows.

The following example sets the protected VLANs of the Ethernet ring ERPS1 R-APS VLAN 100 to VLANs 1-99 and 101-2000 in instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 100,1-99,101-2000
Hostname(config-mst)# exit
```

```
Hostname(config)# erps raps-vlan 100
Hostname(config-erps 100)# protected-instance 1
Hostname(config-erps 100)# exit
```

The following example sets the protected VLANs of the Ethernet ring ERPS2 R-APS VLAN 4093 to VLAN 2001-4092 and 4094 in instance 2.

```
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 2 vlan 4093,2001-4092,4094
Hostname(config-mst)# exit
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps 4093)# protected-instance 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps raps-vlan**

1.6 ring-port

Function

Run the **ring-port** command to add ports to an ERPS ring.

Run the **no** form of this command to remove this configuration.

No member port is configured in an ERPS ring by default.

Syntax

ring-port west { *interface-type interface-number* | **virtual-channel** } **east** { *interface-type interface-number* | **virtual-channel** }

no ring-port

Parameter Description

west *interface-type interface-number*: Configures a port as the west port of an ERPS ring.

west virtual-channel: Configures a virtual channel as the west port of an ERPS subring.

east *interface-type interface-number*: Configures a port as the east port of an ERPS ring.

east virtual-channel: Configures a virtual channel as the east port of an ERPS subring.

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

The trunk attributes of a port cannot be modified after the port is added to an ERPS ring.

virtual-channel is only used to configure a port for an ERPS subring.

The ports running ERPS are not involved in the STP calculation. ERPS, Rapid Ethernet Ring Protection (RERP), and Rapid Ethernet Uplink Protection (REUP) do not share ports.

Examples

The following example configures the link mode for Ethernet ring ports.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface tenGigabitEthernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/2)# exit
```

The following example configures TenGigabitEthernet 0/1 as the west port and TenGigabitEthernet 0/2 as the east port, and adds them to R-APS VLAN 4093.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps 4093)# ring-port west tenGigabitEthernet 0/1 east
tenGigabitEthernet 0/2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps enable**

1.7 rpl-port

Function

Run the **rpl-port** command to configure the RPL port for an ERPS ring.

Run the **no** form of this command to remove this configuration.

No RPL port is configured in an ERPS ring by default.

Syntax

rpl-port { **west** | **east** } **rpl-owner**

no rpl-port

Parameter Description

west: Specifies the west port as the RPL port.

east: Specifies the east port as the RPL port.

Default Level

14

Command Modes

R-APS VLAN configuration mode

Usage Guidelines

Each ring must be configured with only one RPL and only one RPL owner node.

For non-RPL owner nodes, the RPL port does not need to be configured. If you need to perform the RPL port, configure it on the port connected to the RPL.

Examples

The following example configures the link mode for Ethernet ring ports in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface tenGigabitEthernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/2)# exit
```

The following example adds the ports to an Ethernet ring in R-APS VLAN configuration mode.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps 4093)# ring-port west tenGigabitEthernet 0/1 east
tenGigabitEthernet 0/2
```

The following example configures the RPL port and RPL owner node.

```
Hostname(config-erps 4093)# rpl-port west rpl-owner
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps raps-vlan**
- **ring-port**

1.8 show erps

Function

Run the **show erps** command to display the parameters and state of ERPS.

Syntax

show erps [{ **global** | **raps-vlan** *vlan-id* [**sub-ring**] }]

Parameter Description

global: Displays global ERPS information.

raps-vlan *vlan-id*: Displays information about a specified R-APS VLAN. The value range of *vlan-id* is from 1 to 4094.

sub-ring: Displays information about a specified subring.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the parameters and state of ERPS.

```
Hostname> enable
Hostname# show erps
ERPS Information
Global Status                : Enabled
Link monitored by               : Not Oam
------------------------------------------
R-APS VLAN                   : 4092
Ring Status                  : Enabled
West Port                    : Te 0/5 (Blocking)
East Port                    : Te 0/7 (Forwarding)
RPL Port                     : West Port
Protected VLANs              : ALL
RPL Owner                    : Enabled
Holdoff Time                 : 0 milliseconds
Guard Time                   : 500 milliseconds
WTR Time                     : 5 minutes
```

```
Current Ring State           : Idle
Associate R-APS VLAN         :
-----------------------------------------
R-APS VLAN                   : 4093
Ring Status                  : Enabled
West Port                    : Virtual Channel
East Port                    : Te 0/10 (Forwarding)
RPL Port                     : None
Protected VLANs              : ALL
RPL Owner                    : Disabled
Holdoff Time                 : 0 milliseconds
Guard Time                   : 500 milliseconds
WTR Time                     : 5 minutes
Current Ring State           : Idle
Associate R-APS VLAN         :
-----------------------------------------
R-APS VLAN                   : 4094
Ring Status                  : Enabled
West Port                    : Virtual Channel
East Port                    : Te 0/12 (Forwarding)
RPL Port                     : None
Protected VLANs              : ALL
RPL Owner                    : Disabled
Holdoff Time                 : 0 milliseconds
Guard Time                   : 500 milliseconds
WTR Time                     : 5 minutes
Current Ring State           : Idle
Associate R-APS VLAN         :
Hostname# show erps raps-vlan 4093 sub-ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs    TC Propagation State
------------------    --------------------None
100                   Enable
200                   Enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps enable**

1.9 state enable

Function

Run the **state enable** command to enable the ERPS function for a specified ring.

Run the **no** command to disable this feature.

The ERPS function of an Ethernet ring is disabled by default.

Syntax

state enable

no state enable

Parameter Description

N/A

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

ERPS takes effect in a specified ring only after ERPS is enabled both globally and for the ring.

Examples

The following example configures the link mode for Ethernet ring ports in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface tenGigabitEthernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/2)# exit
```

The following example adds the ports to an Ethernet ring in R-APS VLAN configuration mode.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps 4093)# ring-port west tenGigabitEthernet 0/1 east
tenGigabitEthernet 0/2
```

The following example enables the ERPS function for the specified ring.

```
Hostname(config-erps 4093)# state enable
```

The following example enables the ERPS function globally.

```
Hostname(config-erps 4093)# exit
Hostname(config)# erps enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps raps-vlan**
- **ring-port**

1.10 sub-ring tc-propagation

Function

Run the **sub-ring tc-propagation** command to enable the subring topology change notification.

Run the **no** form of this command to disable this feature.

The topology change notification is disabled by default.

Syntax

sub-ring tc-propagation enable

no sub-ring tc-propagation

Parameter Description

N/A

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

This command is configured only on intersecting nodes. After this function is enabled, when the subring topology changes, the intersecting nodes send a topology change notification.

Examples

The following example configures the link mode for Ethernet ring ports in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface tenGigabitEthernet 0/2
```

```
Hostname(config-if-TenGigabitEthernet 0/2)# switchport mode trunk
Hostname(config-if-TenGigabitEthernet 0/2)# exit
```

The following example enters the R-APS VLAN configuration mode and configures ports that need to be added to the Ethernet ring and participate in ERPS calculation.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps4093)# ring-port west tenGigabitEthernet 0/1 east
tenGigabitEthernet 0/2
```

The following example configures an Ethernet subring.

```
Hostname(config)# erps raps-vlan 100
Hostname(config)# interface tenGigabitEthernet 0/3
Hostname(config-if-TenGigabitEthernet 0/3)# switchport mode trunk
Hostname(config-if-GTenGigabitEthernet 0/3)# exit
Hostname(config)# erps raps-vlan 100
Hostname(config-erps 100)# ring-port west tenGigabitEthernet 0/3 east virtual-channel
```

The following example associates the subring with the other Ethernet ring.

```
Hostname(config-erps 100)# associate sub-ring raps-vlan 4093
```

The following example enables the subring topology change notification.

```
Hostname(config-erps 100)# sub-ring tc-propagation enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps raps-vlan**
- **ring-port**

1.11 timer

Function

Run the **timer** command to configure ERPS timers.

Run the **no** form of this command to restore the default configuration.

By default, the time from a failure to the protection switching of a device is 0 milliseconds, the time from failure recovery to a response to SF R-APS packets is 500 milliseconds, and the time from failure recovery and reblocking of the RPL owner port is 2 minutes.

Syntax

timer { **holdoff-time** *holdoff* | **guard-time** *guard* | **wtr-time** *wtr* }

no timer { **holdoff-time** | **guard-time** | **wtr-time** }

Parameter Description

holdoff-time *holdoff*: Indicates the Holdoff timer, which controls the time from a failure to protection switching of a device, in 100 milliseconds. The value range is from 0 to 100. The default value is **0**. When a failure occurs, the Holdoff timer is started. After the timer times out, if the failure persists, the system reports the failure to ERPS.

guard-time *guard*: Indicates the Guard timer, which controls the time from failure recovery to a response to SF R-APS packets, in 10 milliseconds. The value range is from 1 to 200. The default value is **50**, indicating 500 milliseconds. When a device or link fails, the device will firstly recover the failure, and then send the No Request Ring Auto Protection Switching (NR R-APS) packet to other devices, and start the Guard timer at the same time. The device will respond to the R-APS packet after the timer times out. This timer is used to prevent the device from receiving expired SF R-APS packets.

wtr-time *wtr*: Indicates the Wait to Restore (WTR) timer, which controls the time from failure recovery to reblocking of the RPL owner port, in minutes. The value range is from 1 to 12. The default value is **2**. When an Ethernet ring is in good conditions, the RPL owner port is blocked to prevent loops in the network. If a device or link fails in an Ethernet ring, the RPL owner port will be unblocked. If these device or link failures are recovered, the RPL owner port can be blocked again after a certain period of time. The purpose is to prevent link flapping caused by some ports not recovered to the up state during link recovery.

Command Modes

R-APS VLAN configuration mode

Default Level

14

Usage Guidelines

The Holdoff timer is used to minimize frequent ERPS topology switching due to intermittent link failures. After you configure the Holdoff timer, ERPS performs topology switching only if the link failure still persists after the timer times out.

The Guard timer is used to prevent a device from receiving expired R-APS messages. When the device detects that a link failure is cleared, it sends link recovery packets and starts the Guard timer. Before the Guard timer expires, all packets except Flush packets indicating a subring topology change will be discarded.

The WTR timer is effective only for RPL owner nodes. It is used to avoid ring status misjudgment by the RPL owner node. When an RPL owner node detects that a failure is cleared, it will not perform topology switching immediately but only if the Ethernet ring is recovered after the WTR timer times out. If a ring failure is detected again before the timer expires, the RPL owner node cancels the timer and does not perform topology switching.

Examples

The following example displays the default values of the ERPS timers before configuration in R-APS VLAN configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# erps raps-vlan 4093
```

```
Hostname(config-erps 4093)# show erps
ERPS Information
Global Status             : Disabled
Link monitored by         : Not Oam
-----------------------------------------
R-APS VLAN               : 4093
Ring Status              : Disabled
West Port                : None
East Port                : None
RPL Port                 : None
Protected VLANs           : None
RPL Owner                : Disabled
Holdoff Time             : 0 milliseconds
Guard Time               : 500 milliseconds
WTR Time                 : 2 minutes
Current Ring State        : initialize
Associate R-APS VLAN      :
```

The following example configures the ERPS timers.

```
Hostname(config-erps 4093)# timer holdoff-time 10
Hostname(config-erps 4093)# timer guard-time 10
Hostname(config-erps 4093)# timer wtr-time 10
```

The example displays the configured values of the ERPS timers.

```
Hostname(config-erps 4093)#show erps
ERPS Information
Global Status             : Disabled
Link monitored by         : Not Oam
-----------------------------------------
R-APS VLAN               : 4093
Ring Status              : Disabled
West Port                : None
East Port                : None
RPL Port                 : None
Protected VLANs           : None
RPL Owner                : Disabled
Holdoff Time             : 1000 milliseconds
Guard Time               : 100 milliseconds
WTR Time                 : 10 minutes
Current Ring State        : initialize
Associate R-APS VLAN      :
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **erps raps-vlan**

1 LLDP Commands

Command	Function
civic-location	Configure Link Layer Discovery Protocol (LLDP) civic address information.
clear lldp statistics	Clear LLDP statistics.
clear lldp table	Clear the neighbor information of LLDP.
device-type	Configure a device type.
lldp compliance vendor	Enable the compatibility with the neighbor discovery of vendors' devices.
lldp enable	Enable the LLDP function.
lldp encapsulation snap	Set the LLDP packet encapsulation format to Subnetwork Access Protocol (SNAP).
lldp error-detect	Enable the LLDP error detection function.
lldp fast-count	Configure the number of LLDP packets that can be transmitted rapidly.
lldp hold-multiplier	Configure the time to live (TTL) multiplier for LLDP packets.
lldp ignore pvid-error-detect	Enable the function of ignoring the port VLAN ID (PVID) detection.
lldp location civic-location identifier	Configure the civic address in LLDP-MED TLVs.
lldp location elin identifier	Configure the emergency telephone number to be encapsulated in the Location Identification TLV.
lldp management-address-tlv	Configure the management address to be advertised in an LLDP packet.
lldp mode	Configure the LLDP work mode.
lldp network-policy profile	Create an LLDP network policy and enter the LLDP network policy configuration mode.
lldp notification remote-change enable	Enable the LLDP trap function.
lldp timer notification-interval	Configure the LLDP trap transmission interval.
lldp timer reinit-delay	Configure an LLDP interface initialization delay.

lldp timer tx-delay	Configure an LLDP packet transmission delay.
lldp timer tx-interval	Configure an LLDP packet transmission interval.
lldp tlv-enable	Configure the types of TLVs to be advertised.
show lldp local-information	Display the LLDP information on the local device, which will be organized as TLVs and sent to neighbors.
show lldp location	Display the LLDP civic address or emergency telephone number of the local device.
show lldp neighbors	Display the LLDP information of a neighbor received by an interface.
show lldp network-policy	Display the LLDP network policy configuration of the local device.
show lldp statistics	Display the LLDP statistics.
show lldp status	Display the LLDP status.
show lldp tlv-config	Display the configuration of TLVs to be advertised by an interface.
voice vlan	Configure an LLDP network policy, in which the application type is specified for a voice VLAN.

1.1 civic-location

Function

Run the **civic-location** command to configure Link Layer Discovery Protocol (LLDP) civic address information.

Run the **no** form of this command to remove this configuration.

No address information is configured by default.

Syntax

{ **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*

no { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** }

Parameter Description

Parameters of this command consist of two parts: address type indicated by *ca-type* and address information indicated by *ca-word***.** The **civic-location** keyword is not reflected in the configuration command. The configuration starts directly with the *ca-type* parameter. Run the *ca-type ca-word* command to configure the device address, or run the **no** form of this command to delete the corresponding address information.

- Optional parameters for *ca-type* include the following:

  country (country);

  state (state, the CA type is 1);

  county (county, the CA type is 2);

  city (city, the CA type is 3);

  division (district, the CA type is 4);

  neighborhood (community, the CA type is 5);

  street-group (street, the CA type is 6);

  leading-street-dir (street No., the CA type is 16);

  trailing-street-suffix (street No., the CA type is 17);

  street-suffix (street No., the CA type is 18);

  number (street No., the CA type is 19);

  street-number-suffix (street No., the CA type is 20);

  landmark (landmark, the CA type is 21);

  additional-location-information (additional address, the CA type is 22);

  name (name, the CA type is 23);

  postal-code (postal code, the CA type is 24);

building (building, the CA type is 25);

unit (unit, the CA type is 26);

floor (floor, the CA type is 27);

room (room, the CA type is 28);

type-of-place (place type, the CA type is 29);

postal-community-name (post office, the CA type is 30);

post-office-box (post office box, the CA type is 31);

additional-code (additional code, the CA type is 32).

- Fill specific information in *ca-word*.

  When the address type is **country**, only two characters can be used to represent a country. For example, CH represents China.

Command Modes

LLDP civic address configuration mode

Default Level

14

Usage Guidelines

Run the **lldp location civic-location identifier** *id* command to enter the LLDP civic address configuration mode.

In LLDP civic address configuration mode, run the **civic-location** command to configure the civic address information for the device.

Examples

The following example configures the LLDP civic address information, in which **LLDP Civic Address ID** is set to **1**, **Country** is set to **CH**, and **City** is set to **Fuzhou**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# country CH
Hostname(config-lldp-civic)# city Fuzhou
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**
- **lldp location civic-location identifier**

1.2 clear lldp statistics

Function

Run the **clear lldp statistics** command to clear LLDP statistics.

Syntax

clear lldp statistics [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

When the **interface** parameter is specified, this command will clear the LLDP statistics of the specified interface.

Examples

The following example clears the LLDP statistics of TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear lldp statistics interface tenGigabitEthernet 0/1
Hostname# show lldp statistics interface tenGigabitEthernet 0/1
Lldp statistics information of port [TenGigabitEthernet 0/1]
The number of lldp frames transmitted      : 0
The number of frames discarded            : 0
The number of error frames                : 0
The number of lldp frames received         : 0
The number of TLVs discarded              : 0
The number of TLVs unrecognized           : 0
The number of neighbor information aged out : 0
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**
- **show lldp statistics**

1.3 clear lldp table

Function

Run the **clear lldp table** command to clear the neighbor information of LLDP.

Syntax

clear lldp table [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

When the **interface** parameter is specified, this command will clear the LLDP neighbor information of the specified interface. When the **interface** parameter is not specified, this command will clear the LLDP neighbor information of all interfaces.

Examples

The following example clears the LLDP neighbor information of TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear lldp table interface tenGigabitEthernet 0/1
Hostname# show lldp neighbors interface tenGigabitEthernet 0/1
Hostname# show lldp neighbors interface tenGigabitEthernet 0/1
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
System Name        Local Intf        Port ID              Capability   Aging-time
Total entries displayed: 0
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.4 device-type

Function

Run the **device-type** command to configure a device type.

Run the **no** form of this command to remove this configuration.

No device type is configured by default.

Syntax

device-type *device-type*

no device-type

Parameter Description

device-type: Device type. The value range is from 0 to 2. The value **0** indicates that the device type is DHCP server, **1** indicates that the device type is switch, and **2** indicates that the device type is LLDP- MED terminal. The default value is empty.

Command Modes

LLDP civic address configuration mode

Default Level

14

Usage Guidelines

After entering the LLDP civic address configuration mode, configure the device type.

Examples

The following example sets the device type to switch and displays the configuration result.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# device-type 1
Hostname(config-lldp-civic)# show lldp location civic-location identifier 1
civic location information:
--------------------------
Identifier          :1
device type         :1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**
- **lldp location civic-location identifier**

1.5 lldp compliance vendor

Function

Run the **lldp compliance vendor** command to enable the compatibility with the neighbor discovery of vendors' devices.

Run the **no** form of this command to disable this feature.

The compatibility with the neighbor discovery of vendors' devices is disabled by default.

Syntax

lldp compliance vendor

no lldp compliance vendor

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the compatibility with the neighbor discovery of vendors' devices globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp compliance vendor
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.6 lldp enable

Function

Run the **lldp enable** command to enable the LLDP function.

Run the **no** form of this command to disable this feature.

The LLDP function is enabled by default.

Syntax

lldp enable

no lldp enable

Parameter Description

N/A

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

LLDP takes effect only after it is enabled globally and on an interface.

Examples

The following example disables the LLDP function globally and on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no lldp enable
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no lldp enable
```

Notifications

N/A

Common Errors

The LLDP function is enabled on an interface but disabled globally. As a result, the LLDP function does not take effect.

An interface can learn a maximum of five neighbors.

If a neighbor does not support LLDP but it is connected to an LLDP-supported device in the downlink direction, an interface may learn information about the device that is not directly connected to the interface because the neighbor may forward LLDP packets.

Platform Description

N/A

Related Commands

N/A

1.7 lldp encapsulation snap

Function

Run the **lldp encapsulation snap** command to set the LLDP packet encapsulation format to Subnetwork Access Protocol (SNAP).

Run the **no** form of this command to restore the default configuration.

The default LLDP packet encapsulation format is Ethernet II.

Syntax

lldp encapsulation snap

no lldp encapsulation snap

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The same LLDP packet encapsulation format must be configured on a device and its neighbors to ensure their normal communication.

Examples

The following example sets the LLDP packet encapsulation format to SNAP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp encapsulation snap
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.8 lldp error-detect

Function

Run the **lldp error-detect** command to enable the LLDP error detection function.

Run the **no** form of this command to disable this feature.

The LLDP error detection function is enabled by default.

Syntax

lldp error-detect

no lldp error-detect

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

LLDP error detection function includes detecting the VLAN configuration at both ends of a link, interface status, aggregate port configuration, MTU configuration, and loops. When LLDP detects an error, an alarm is generated to alert administrators.

The LLDP error detection function relies on the specific Type, Length, Value (TLV) in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure that LLDP error detection functions properly.

Examples

The following example enables the LLDP error detection function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp error-detect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.9 lldp fast-count

Function

Run the **lldp fast-count** command to configure the number of LLDP packets that can be transmitted rapidly.

Run the **no** form of this command to remove this configuration.

By default, three LLDP packets are transmitted rapidly.

Syntax

lldp fast-count *fast-count-value*

no lldp fast-count

Parameter Description

fast-count-value: Number of LLDP packets that can be transmitted rapidly. The value range is from 1 to 10, and the default value is **3**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When LLDP discovers a new neighbor or the LLDP work mode is changed from disabled or Rx to TxRx or Tx, the fast transmission mechanism is started so that the neighbor quickly learns the information of the device. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval.

Examples

The following example sets the number of LLDP packets that can be transmitted rapidly to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp fast-count 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.10 lldp hold-multiplier

Function

Run the **lldp hold-multiplier** command to configure the time to live (TTL) multiplier for LLDP packets.

Run the **no** form of this command to remove this configuration.

The default TTL multiplier of LLDP packets is **4**.

Syntax

lldp hold-multiplier *ttl-value*

no lldp hold-multiplier

Parameter Description

ttl-value: TTL multiplier of LLDP packets. The value range is from 2 to 10, and the default value is **4**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In an LLDP packet, the value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier × Packet transmission interval + 1. You can control the TTL of the local device information on neighbors by adjusting the TTL multiplier.

Examples

The following example sets the TTL multiplier to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp hold-multiplier 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.11 lldp ignore pvid-error-detect

Function

Run the **lldp ignore pvid-error-detect** command to enable the function of ignoring the port VLAN ID (PVID) detection.

Run the **no** form of this command to disable this feature.

The function of ignoring PVID detection is disabled by default.

Syntax

lldp ignore pvid-error-detect

no lldp ignore pvid-error-detect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of ignoring the PVID detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp ignore pvid-error-detect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.12 lldp location civic-location identifier

Function

Run the **lldp location civic-location identifier** command to configure the civic address in LLDP-MED TLVs.

Run the **no** form of this command to remove this configuration.

Syntax

lldp location civic-location identifier *id*

no lldp location civic-location identifier *id*

Parameter Description

id: Identifier of a civic address for a network device. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enter the LLDP civic address configuration mode.

You can create a civic address for a network device in LLDP civic address configuration mode.

Examples

The following example configures the civic address in LLDP-MED TLVs, and sets the ID to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.13 lldp location elin identifier

Function

Run the **lldp location elin identifier** command to configure the emergency telephone number to be encapsulated in the Location Identification TLV.

Run the **no** form of this command to remove this configuration.

Syntax

lldp location elin identifier *id* **elin-location** *tel-number*

no lldp location elin identifier *id*

Parameter Description

id: Identifier of an emergency telephone number. The value range is from 1 to 1024.

tel-number: Emergency telephone number, in bytes. The value range is from 10 to 25.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **show lldp location elin-location** { **identifier** *id* | **interface** *interface-type interface-number* | **static** } command is used to display the configuration result.

Examples

The following example configures the emergency telephone number to be encapsulated in the Location Identification TLV.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location elin identifier 1 elin-location 085283671111
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.14 lldp management-address-tlv

Function

Run the **lldp management-address-tlv** command to configure the management address to be advertised in an LLDP packet.

Run the **no** form of this command to remove this configuration.

By default, the management address to be advertised in an LLDP packet is the IPv4 address of the minimum VLAN supported by the interface. If no IPv4 address is configured for the VLAN with the minimum ID, LLDP keeps searching the other VLANs with the minimum ID until a qualified IPv4 address is obtained. If no IPv4 address is found, LLDP searches the IPv6 address of the minimum VLAN supported by the interface. If no IPv6 address is found, the local address 127.0.0.1 is used as the management address to be advertised.

Syntax

lldp management-address-tlv { *ipv4-address* | *ipv6-address* }

no lldp management-address-tlv

Parameter Description

ipv4-address: IPv4 management address to be advertised in an LLDP packet.

ipv6-address: IPv6 management address to be advertised in an LLDP packet.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the management address to be advertised in an LLDP packet to **192.168.1.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp management-address-tlv 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.15 lldp mode

Function

Run the **lldp mode** command to configure the LLDP work mode.

Run the **no** form of this command to remove this configuration.

The default LLDP work mode is **TxRx**, that is, an interface transmits and receives LLDPDUs.

Syntax

lldp mode { **tx** | **rx** | **txrx** }

no lldp mode

Parameter Description

tx: Only transmits LLDPDUs.

rx: Only receives LLDPDUs.

txrx: Transmits and receives LLDPDUs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the LLDP work mode of an interface is disabled, the interface neither transmits nor receives LLDP packets.

To make LLDP take effect on an interface, make sure to enable LLDP globally and set the LLDP work mode of the interface to **Tx**, **Rx** or **TxRx**.

Examples

The following example sets the LLDP work mode of an interface to **Tx**, that is, the interface can only transmit LLDPDUs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp mode tx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.16 lldp network-policy profile

Function

Run the **lldp network-policy profile** command to create an LLDP network policy and enter the LLDP network policy configuration mode.

Run the **no** form of this command to remove this configuration.

No LLDP network policy is configured by default.

Syntax

lldp network-policy profile *profile-number*

no lldp network-policy profile *profile-number*

Parameter Description

profile-number: ID of an LLDP network policy. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enter the LLDP network policy mode after specifying a policy ID.

After entering the LLDP network policy mode, you can run the **voice vlan** command to configure a specific network policy.

Examples

The following example creates an LLDP network policy, with the policy ID of 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp network-policy profile 1
Hostname(config-lldp-network-policy)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.17 lldp notification remote-change enable

Function

Run the **lldp notification remote-change enable** command to enable the LLDP trap function.

Run the **no** form of this command to disable this feature.

The LLDP trap function is disabled by default.

Syntax

lldp notification remote-change enable

no lldp notification remote-change enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The LLDP trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance.

Examples

The following example enables the LLDP trap function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp notification remote-change enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.18 lldp timer notification-interval

Function

Run the **lldp timer notification-interval** command to configure the LLDP trap transmission interval.

Run the **no** form of this command to remove this configuration.

The default LLDP trap transmission interval is 5 seconds.

Syntax

lldp timer notification-interval *trap*

no lldp timer notification-interval

Parameter Description

trap: LLDP trap transmission interval, in seconds. The value range is from 5 to 3600, and the default value is **5**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can configure an LLDP trap transmission interval to prevent frequent transmission of LLDP trap messages. LLDP changes detected within this interval will be transmitted to the NMS server through traps.

Examples

The following example sets the LLDP trap transmission interval to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp timer notification-interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.19 lldp timer reinit-delay

Function

Run the **lldp timer reinit-delay** command to configure an LLDP interface initialization delay.

Run the **no** form of this command to remove this configuration.

The default LLDP interface initialization delay is **2** seconds.

Syntax

lldp timer reinit-delay *reinit*

no lldp timer reinit-delay

Parameter Description

reinit: LLDP interface initialization delay, in seconds. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An interface initialization delay can be configured to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Examples

The following example sets the LLDP interface initialization delay to 3 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp timer reinit-delay 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.20 lldp timer tx-delay

Function

Run the **lldp timer tx-delay** command to configure an LLDP packet transmission delay.

Run the **no** form of this command to remove this configuration.

The default LLDP packet transmission delay is **2** seconds.

Syntax

lldp timer tx-delay *txdelay*

no lldp timer tx-delay

Parameter Description

txdelay: LLDP packet transmission delay, in seconds. The value range is from 1 to 8192.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Examples

The following example sets the LLDP packet transmission delay to 3 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp timer tx-delay 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.21 lldp timer tx-interval

Function

Run the **lldp timer tx-interval** command to configure an LLDP packet transmission interval.

Run the **no** form of this command to remove this configuration.

The default LLDP packet transmission interval is **30** seconds.

Syntax

lldp timer tx-interval *txinterval*

no lldp timer tx-interval

Parameter Description

txinterval: LLDP packet transmission interval, in seconds. The value range is from 1 to 32768.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the LLDP packet transmission interval to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp timer tx-interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.22 lldp tlv-enable

Function

Run the **lldp tlv-enable** command to configure the types of TLVs to be advertised.

Run the **no** form of this command to remove this configuration.

By default, if a device supports the Data Center Bridging Capability Exchange protocol (DCBX), interfaces are allowed to transmit all types of TLVs except IEEE 802.3 organizationally specific TLVs and LLDP-MED TLVs. If a device does not support DCBX, interfaces are allowed to transmit all types of TLVs except the Location Identification TLV. The default transmission policy is none for the Network Policy TLV in LLDP-MED TLVs.

Syntax

lldp tlv-enable *tlv-type subtype*

no lldp tlv-enable *tlv-type subtype*

Parameter Description

tlv-type: TLV type. The value range is **basic-tlv**, **dot1-tlv**, **dot3-tlv**, and **med-tlv**. One of these types must be configured.

subtype: Sub-type. One sub-type must be configured. The sub-type varies with *tlv-type*.

- The value range of *subtype* for **basic-tlv** (basic management TLVs) is as follows:
  - **all**: Advertises all optional TLVs of this type.
  - **port-description**: Indicates the Port Description TLV.
  - **system-capability**: Indicates the System Capabilities TLV.
  - **system-description**: Indicates the System Description TLV.
  - **system-name**: Indicates the System Name TLV.
- The value range of *subtype* for **dot1-tlv** (802.1 organizationally specific TLVs) is as follows:
  - **all**: Advertises all optional TLVs of this type.
  - **port-vlan-id:** Indicates the Port VLAN ID TLV.
  - **protocol-vlan-id** [*vlan-id*]: Indicates the Port And Protocol VLAN ID TLV. Where, *vlan-id* indicates the port protocol VLAN ID. The value range is from 1 to 4094.
  - **vlan-name** [*vlan-id*]: Indicates the VLAN Name TLV. Where, *vlan-id* indicates the VLAN ID. The value range is from 1 to 4094.
- The value range of *subtype* for **dot3-tlv** (802.3 organizationally specific TLVs) is as follows:
  - **all**: Advertises all optional TLVs of this type.
  - **link-aggregation**: Indicates the Link Aggregation TLV.
  - **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV.
  - **max-frame-size**: Indicates the Maximum Frame Size TLV.
  - **power**: Indicates the Power Via MDI TLV.
- The value range of *subtype* for **med-tlv** (LLDP MED TLVs) is as follows:
  - **all**: Advertises all types of LLDP-MED TLVs other than the **Location** Identification TLV.
  - **capability**: Indicates the LLDP-MED Capabilities TLV.
  - **inventory:** Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier.
  - **location** { **civic-location | elin** } **identifier** *id*: Indicates the Location Identification TLV. **civic-location**

indicates the civic address information of the network connectivity device to be encapsulated, **elin** indicates the emergency telephone number to be encapsulated, and **identifier** *id* indicates the policy ID, with the value range from 1 to 1024.

- **network-policy profile** [*profile-num*]: Indicates the Network Policy TLV. Where, *profile-num* indicates the network policy ID. The value range is from 1 to 1024.
- **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- If you configure the **all** parameter for the basic management TLVs, IEEE 802.1 organizationally specific TLVs, and IEEE 802.3 organizationally specific TLVs, all optional TLVs of these types are advertised.
- If you configure the **all** parameter for the LLDP-MED TLVs, all LLDP-MED TLVs except the Location Identification TLV are advertised.
- If you want to configure the LLDP-MED **capability** TLV, configure the LLDP IEEE 802.3 **mac-physic** TLV first. If you want to cancel the LLDP IEEE 802.3 **mac-physic** TLV, cancel the LLDP-MED **capability** TLV first.
- If you want to configure LLDP-MED TLVs, configure the LLDP-MED **capability** TLV before configuring other types of LLDP-MED TLVs. If you want to cancel the advertisement of LLDP-MED TLVs, cancel the LLDP-MED **capability** TLV before canceling other types of LLDP-MED TLVs. If a device is connected to an IP phone in the downlink direction and the IP phone supports LLDP-MED, you can configure the Network Policy TLV to deliver policies to the IP phone.

Examples

The following example configures the advertisement of all optional IEEE 802.1 organizationally specific TLVs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# lldp tlv-enable dot1-tlv all
```

The following example applies the LLDP network policy 1 to TenGigabitEthernet 0/1.

```
Hostname(config-if-TenGigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy
profile 1
```

The following example applies the LLDP civic address configuration to TenGigabitEthernet 0/1.

```
Hostname(config-if-TenGigabitEthernet 0/1)# lldp tlv-enable med-tlv location
civic-location identifier 1
```

The following example applies the emergency telephone number to TenGigabitEthernet 0/1.

```
Hostname(config-if-TenGigabitEthernet 0/1)# lldp tlv-enable med-tlv location elin
identifier 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.23 show lldp local-information

Function

Run the **show lldp local-information** command to display the LLDP information on the local device, which will be organized as TLVs and sent to neighbors.

Syntax

show lldp local-information [**global** | **interface** *interface-type interface-number*]

Parameter Description

global: Displays the global LLDP information to be transmitted.

interface *interface-type interface-number*: Displays the LLDP information of a specified interface type and number to be transmitted.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is specified, all the LLDP information will be displayed, including the global and interface LLDP information.

Examples

The following example displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.

```
Hostname> enable
Hostname# show lldp local-information
Global LLDP local-information:
  Chassis ID type               : MAC address
  Chassis id                    : 00d0.f822.33aa
  System name                   : System name
```

```
  System description              : System description
  System capabilities supported    : Repeater, Bridge, Router
  System capabilities enabled      : Repeater, Bridge, Router
  LLDP-MED capabilities           : LLDP-MED Capabilities, Network Policy, Location
Identification, Extended Power via MDI-PD, Inventory
  Device class                   : Network Connectivity
  HardwareRev                    : 1.0
  FirmwareRev                    :
  SoftwareRev                    :
  SerialNum                      : 1234942570001
  Manufacturer name               : Manufacturer name
  Asset tracking identifier       :
------------------------------------------------------------------------------
LLDP local-information of port [TenGigabitEthernet 0/1]
------------------------------------------------------------------------------
  Port ID type                   : Interface name
  Port id                        : TenGigabitEthernet 0/1
  Port description               :
  Management address subtype       : 802 mac address
  Management address              : 00d0.f822.33aa
  Interface numbering subtype      :
  Interface number               : 0
  Object identifier              :
  802.1 organizationally information
  Port VLAN ID                   : 1
  Port and protocol VLAN ID(PPVID)  : 1
     PPVID Supported             : YES
     PPVID Enabled               : NO
  VLAN name of VLAN 1             : VLAN0001
  Protocol Identity              :
  802.3 organizationally information
  Auto-negotiation supported       : YES
  Auto-negotiation enabled        : YES
  PMD auto-negotiation advertised   :
  Operational MAU type            : Speed(100)/Duplex(Half)
  PoE support                    : NO
  Link aggregation supported       : YES
  Link aggregation enabled        : NO
  Aggregation port ID             : 0
  Maximum frame Size              : 1500
  LLDP-MED organizationally information
  Power-via-MDI device type        : PD
  Power-via-MDI power source       : Local
  Power-via-MDI power priority     :
  Power-via-MDI power value        :
  Model name                     : Model name
```

Table 1-1 Output Fields of the show lldp local-information Command

Field	Description
Chassis ID type	Chassis ID type, used to identify the **Chassis ID** field.
Chassis ID	Device ID, represented using a MAC address.
System name	Device name.
System description	Device description, including the hardware version, software version, and operating system information.
System capabilities supported	Functions supported by the system.
System capabilities enabled	Functions enabled in the system.
LLDP-MED capabilities	LLDP-MED capabilities supported by the system.
Device class	MED device type. There are two types: network connectivity device and terminal device. ● Network connectivity device: Network connection device. ● Class I: General terminal device. ● Class II: Media terminal device, which supports the capabilities of class I devices and media streaming. ● Class III: Communication terminal device, which supports the capabilities of class I and class II devices, and IP communication.
HardwareRev	Hardware version.
FirmwareRe	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Manufacturer.
Asset tracking identifier	Asset identifier.
Port ID type	Port ID type.
Port ID	Port ID.
Port description	Port descriptor.
Management address subtype	Management address type.
Management address	Management address.

Field	Description
Interface numbering subtype	Management address interface type.
Interface number	Management address interface ID.
Object identifier	Management address object identifier.
Port VLAN ID	Port VLAN ID.
Port and protocol VLAN ID	Port and protocol VLAN ID.
PPVID Supported	Whether the port and protocol VLAN is supported. ● Yes: Supported. ● No: Not supported.
PPVID Enabled	Whether the port and protocol VLAN is enabled. ● Yes: Enabled. ● No: Disabled.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol Identity	Protocol identifier.
Auto-negotiation supported	Whether auto-negotiation is supported. ● Yes: Supported. ● No: Not supported.
Auto-negotiation enabled	Whether auto-negotiation is enabled. ● Yes: Enabled. ● No: Disabled.

Field	Description
PMD auto-negotiation advertised	Auto-negotiation capability advertised by the interface: ● 1000BASE-T(FD) ● 1000BASE-T(HD) ● 1000BASE-X, -LX, -SX, -CX(FD) ● 1000BASE-X, -LX, -SX, -CX(HD) ● Asymmetric and Symmetric PAUSE(FD) ● Symmetric PAUSE(FD) ● Asymmetric PAUSE(FD) ● PAUSE(FD) ● 100BASE-T2(FD) ● 100BASE-T2(HD) ● 100BASE-TX(FD) ● 100BASE-TX(HD) ● 100BASE-T4 ● 10BASE-T(FD) ● 10BASE-T(HD) ● Other: Capability other than values above.
Operational MAU type	Interface auto-negotiation rate and duplex mode.
PoE support	Whether PoE is supported. ● Yes: Supported. ● No: Not supported.
Link aggregation supported	Whether link aggregation is supported. ● Yes: Supported. ● No: Not supported.
Link aggregation enabled	Whether link aggregation is enabled. ● Yes: Enabled. ● No: Disabled.
Aggregation port ID	Link aggregation port ID.
Maximum frame Size	Maximum frame length supported by an interface.
Power-via-MDI device type	Device type, including power sourcing equipment (PSE) and powered device (PD).
Power-via-MDI power source	Power supply type.

Field	Description
Power-via-MDI power priority	Power supply priority.
Power-via-MDI power value	Interface power.
Model name	Module name.

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.24 show lldp location

Function

Run the **show lldp location** command to display the LLDP civic address or emergency telephone number of the local device.

Syntax

show lldp location { **civic-location** | **elin-location** } { **identifier** *id* | **interface** *interface-type interface-number* | **static** }

Parameter Description

civic-location: Indicates the encapsulated civic address information of the network connectivity device.

elin-location: Indicates the encapsulated emergency telephone number.

identifier *id*: Displays the address or emergency telephone number configured by users in a policy of a specified policy ID. The value range is from 1 to 1024.

interface *interface-type interface-number*: Displays the address or emergency telephone number on a specified interface. *interface-type interface-number* indicates the interface type and number.

static: Displays all addresses or emergency telephone numbers configured by users.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If a policy ID is specified, the specific address or emergency telephone number will be displayed.

If an interface type and number are specified, the address and emergency telephone configured for this interface will be displayed.

If no parameter is specified, all addresses or emergency telephone numbers will be displayed.

Examples

The following example displays the LLDP civic address configured for the local device.

```
Hostname> enable
Hostname# show lldp location civic-location static
Civic location information
------------------------------------------------
Identifier              : 1
County                  : CH
City Division           : fuzhou
Leading street direction: 44
Street number           : 68
Landmark                : 233
Name                    : liuy
Building                : 19bui
Floor                   : 1
Room                    : 33
City                    : fuzhou
Country                 : 86
Additional location     : aaa
Ports                   : Te0/1
-----------------------------------
Identifier              : tee
-----------------------------------
```

The following example displays the emergency telephone number of the local device.

```
Hostname# show lldp location elin-location static
Elin location information
--------------------------
Identifier : t
Elin      : iiiiiiiiii
Ports     : Te1/0/3
--------------------------
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**
- **lldp location civic-location identifier**
- **lldp location elin identifier**

1.25 show lldp neighbors

Function

Run the **show lldp neighbors** command to display the LLDP information of a neighbor received by an interface.

Syntax

show lldp neighbors [**interface** *interface-type interface-number*] [**detail**]

Parameter Description

interface *interface-type interface-number*: Displays the LLDP information of a neighbor received by a specified interface. If this parameter is not specified, the LLDP information received by all interfaces is displayed.

detail: Displays the details about a neighbor. If this parameter is not specified, the neighbor summary is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is specified, the LLDP summaries of neighbors received by all interfaces are displayed.

Examples

The following example displays the LLDP details of neighbors received by all interfaces.

```
Hostname> enable
Hostname# show lldp neighbors detail
------------------------------------------------------------------
LLDP neighbor-information of port [TenGigabitEthernet 0/1]
------------------------------------------------------------------
  Neighbor index                : 1
  Device type                   : LLDP Device
  Update time                   : 1hour 53minutes 30seconds
Aging time                       : 5seconds
  Chassis ID type               : MAC address
  Chassis id                    : 00d0.f822.33cd
  System name                   : System name
  System description             : System description
  System capabilities supported    : Repeater, Bridge, Router
```

```
  System capabilities enabled      : Repeater, Bridge, Router
  Management address subtype       : 802 mac address
  Management address              : 00d0.f822.33cd
  Interface numbering subtype      :
  Interface number                : 0
  Object identifier               :
  LLDP-MED capabilities           :
  Device class                    :
  HardwareRev                     :
  FirmwareRev                     :
  SoftwareRev                     :
  SerialNum                       :
  Manufacturer name               :
  Asset tracking identifier       :
  Port ID type                    : Interface name
  Port id                         : TenGigabitEthernet 0/1
  Port description                :
  802.1 organizationally information
  Port VLAN ID                    : 1
  Port and protocol VLAN ID(PPVID)  : 1
     PPVID Supported              : YES
     PPVID Enabled                : NO
  VLAN name of VLAN 1             : VLAN0001
  Protocol Identity               :
  802.3 organizationally information
  Auto-negotiation supported       : YES
  Auto-negotiation enabled         : YES
  PMD auto-negotiation advertised   : 1000BASE-T full duplex mode, 100BASE-TX full
duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half
duplex mode
  Operational MAU type             : speed(1000)/duplex(Full)
  PoE support                     : NO
  Link aggregation supported       : YES
  Link aggregation enabled         : NO
  Aggregation port ID             : 0
  Maximum frame Size              : 1500
  LLDP-MED organizationally information
  Power-via-MDI device type        :
  Power-via-MDI power source       :
  Power-via-MDI power priority     :
Power-via-MDI power value        :
```

Table 1-2 Output Fields of the show lldp neighbors Command

Field	Description
Neighbor index	Neighbor index.

Field	Description
Device type	Neighbor type.
Update time	Last update time of neighbor information.
Aging time	Aging time of neighbor information, namely, the number of seconds after which the neighbor information will be deleted due to aging.
Chassis ID type	Chassis ID type.
Chassis ID	Device ID, represented using a MAC address.
System name	Device name.
System description	Device description, including the hardware version, software version, and operating system information.
System capabilities supported	Functions supported by the system.
System capabilities enabled	Functions enabled in the system.
Management address subtype	Management address type.
Management address	Management address.
Interface numbering subtype	Management address interface type.
Interface number	Management address interface ID.
Object identifier	Management address object identifier.
Device class	MED device type. There are two types: network connectivity device and terminal device. ● Network connectivity device: Network connection device. ● Class I: General terminal device. ● Class II: Media terminal device, which supports the capabilities of class I devices and media streaming. ● Class III: Communication terminal device, which supports the capabilities of class I and class II devices, and IP communication.
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.

Field	Description
Manufacturer name	Manufacturer.
Asset tracking identifier	Asset identifier.
Port ID type	Port ID type.
Port ID	Port ID.
Port description	Port descriptor.
Port VLAN ID	Port VLAN ID.
Port and protocol VLAN ID	Port and protocol VLAN ID.
PPVID Supported	Whether the port and protocol VLAN is supported. ● Yes: Supported. ● No: Not supported.
PPVID Enabled	Whether the port and protocol VLAN is enabled. ● Yes: Enabled. ● No: Disabled.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol Identity	Protocol identifier.
Auto-negotiation supported	Whether auto-negotiation is supported. ● Yes: Supported. ● No: Not supported.
Auto-negotiation enabled	Whether auto-negotiation is enabled. ● Yes: Enabled. ● No: Disabled.

Field	Description
PMD auto-negotiation advertised	Auto-negotiation capability advertised by the interface: ● 1000BASE-T(FD) ● 1000BASE-T(HD) ● 1000BASE-X, -LX, -SX, -CX(FD) ● 1000BASE-X, -LX, -SX, -CX(HD) ● Asymmetric and Symmetric PAUSE(FD) ● Symmetric PAUSE(FD) ● Asymmetric PAUSE(FD) ● PAUSE(FD) ● 100BASE-T2(FD) ● 100BASE-T2(HD) ● 100BASE-TX(FD) ● 100BASE-TX(HD) ● 100BASE-T4 ● 10BASE-T(FD) ● 10BASE-T(HD) ● Other: Capability other than values above.
Operational MAU type	Interface auto-negotiation rate and duplex mode.
PoE support	Whether PoE is supported. ● Yes: Supported. ● No: Not supported.
Link aggregation supported	Whether link aggregation is supported. ● Yes: Supported. ● No: Not supported.
Link aggregation enabled	Whether link aggregation is enabled. ● Yes: Enabled. ● No: Disabled.
Aggregation port ID	Link aggregation port ID.
Maximum frame Size	Maximum frame length supported by an interface.
Power-via-MDI device type	Device type. ● PSE: Power sourcing equipment. ● PD: Powered device.

Field	Description
Power-via-MDI power source	Power supply type.
Power-via-MDI power priority	Power supply priority.
Power-via-MDI power value	Interface power.

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.26 show lldp network-policy

Function

Run the **show lldp network-policy** command to display the LLDP network policy configuration of the local device.

Syntax

show lldp network-policy { **profile** [*profile-num*] | **interface** *interface-type interface-number* }

Parameter Description

profile *profile-num*: Displays the configuration of a specified network policy. The value range of a policy ID is from 1 to 1024.

interface *interface-type interface-number*: Displays the network policy configuration of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is specified, the information about all network policies is displayed.

Examples

The following example displays the LLDP network policy configuration of the local device.

```
Hostname> enable
Hostname# show lldp network-policy profile
network-policy information:
------------------------------------------
Network Policy Profile 1
   voice vlan 2 cos 4 dscp 6
   voice-signaling vlan 2000 cos 4 dscp 6
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.27 show lldp statistics

Function

Run the **show lldp statistics** command to display the LLDP statistics.

Syntax

show lldp statistics [**global** | **interface** *interface-type interface-number*]

Parameter Description

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Displays the LLDP statistics of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is specified, the global LLDP statistics and LLDP statistics of all interfaces are displayed.

Examples

The following example displays the LLDP statistics of all interfaces.

```
Hostname> enable
Hostname# show lldp statistics
lldp statistics global Information:
Neighbor information last changed time     : 1hour 52minute 22second
The number of neighbor information inserted : 2
The number of neighbor information deleted  : 0
```

```
The number of neighbor information dropped  : 0
The number of neighbor information age out  : 1
Lldp statistics information of port [TenGigabitEthernet 0/1]
The number of lldp frames transmitted      : 26
The number of frames discarded            : 0
The number of error frames                : 0
The number of lldp frames received         : 12
The number of TLVs discarded              : 0
The number of TLVs unrecognized           : 0
The number of neighbor information aged out : 0
```

Table 1-3 Output Fields of the show lldp statistics Command

Field	Description
lldp statistics global Information	LLDP global statistics.
Neighbor information last change time	Last update time of neighbor information.
The number of neighbor information inserted	Number of times that neighbor information is updated.
The number of neighbor information deleted	Number of times that neighbor information is deleted.
The number of neighbor information dropped	Number of times that neighbor information is discarded.
The number of neighbor information aged out	Number of timeout times of neighbor information.
Lldp statistics information of port [GigabitEthernet 0/1]	LLDP statistics on the port GigabitEthernet 0/1.
The number of lldp frames transmitted	Number of LLDP frames that are transmitted by the interface.
The number of frames discarded	Number of LLDP frames that are discarded by the interface.
The number of error frames	Number of LLDP error frames occurring on the interface.
The number of lldp frames received	Number of LLDP frames that are received by the interface.
The number of TLVs discarded	Number of LLDP TLVs that are discarded by the interface.
The number of TLVs unrecognized	Number of LLDP TLVs that cannot be recognized by the interface.
The number of neighbor information aged out	Number of timeout times of neighbor information on the interface.

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**
- **clear lldp statistics**

1.28 show lldp status

Function

Run the **show lldp status** command to display the LLDP status.

Syntax

show lldp status [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the LLDP status of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If the **interface** is not specified, the LLDP statuses of all interfaces are displayed.

Examples

The following example displays the LLDP statuses of all interfaces.

```
Hostname> enable
Hostname# show lldp status
Global status of LLDP               : Enable
Neighbor information last changed time : 1hour 52minute 22second
Transmit interval                   : 30s
Hold multiplier                     : 4
Reinit delay                        : 2s
Transmit delay                      : 2s
Notification interval               : 5s
Fast start counts                   : 3
------------------------------------------------------------------
Port [TenGigabitEthernet 0/1]
------------------------------------------------------------------
Port status of LLDP           : Enable
Port state                    : UP
Port encapsulation            : Ethernet II
```

```
Operational mode             : RxAndTx
Notification enable          : NO
Error detect enable          : YES
Number of neighbors          : 1
Number of MED neighbors       : 0
```

Table 1-4 Output Fields of the show lldp status Command

Field	Description
Global status of LLDP	Whether the global LLDP function is enabled. ● Enable: Enabled. ● Disable: Disabled.
Neighbor information last changed time	Last update time of neighbor information.
Transmit interval	LLDP packet transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	Interface initialization delay.
Transmit delay	LLDP packet transmission delay.
Notification interval	LLDP trap transmission interval.
Fast start counts	Number of LLDP packets that are transmitted rapidly.
Port status of LLDP	Whether the LLDP function is enabled on an interface. ● Enable: Enabled. ● Disable: Disabled.
Port state	Interface link state. ● UP: The link is up. ● DOWN: The link is down.
Port encapsulation	LLDP packet encapsulation format.
Operational mode	LLDP work mode.
Notification enable	Whether the LLDP trap function is enabled on an interface. ● Yes: Enabled. ● No: Disabled.
Error detect enable	Whether the error detection function is enabled on an interface. ● Yes: Enabled. ● No: Disabled.
Number of neighbors	Number of neighbors.
Number of MED neighbors	Number of MED neighbors.

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.29 show lldp tlv-config

Function

Run the **show lldp tlv-config** command to display the configuration of TLVs to be advertised by an interface.

Syntax

show lldp tlv-config [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the LLDP TLV configuration of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If the **interface** parameter is not specified, the LLDP TLV configuration of all interfaces is displayed.

Examples

The following example displays the configuration of TLVs to be advertised by interface TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# show lldp tlv-config interface tenGigabitEthernet 0/1
LLDP tlv-config of port [TenGigabitEthernet 0/1]
-------------------------------------------------------------
             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
IEEE 802.3 extend TLV:
MAC-Physic TLV                 YES    YES
Power via MDI TLV               YES    YES
Link Aggregation 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
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

1.30 voice vlan

Function

Run the **voice vlan** command to configure an LLDP network policy, in which the application type is specified for a voice VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** { **voice | voice-signaling** } **vlan** command to restore the default configuration.

No voice VLAN policy is configured by default.

Syntax

{ **voice** | **voice-signaling** } **vlan** { { { *vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*] } | **untagged** | **none** }

no { **voice** | **voice-signaling** } **vlan**

default { **voice | voice-signaling** } **vlan**

Parameter Description

voice: Applies a policy to a voice VLAN.

voice-signaling: Specifies the voice-signaling application type. The function is the same as that of the **voice** command.

{ *vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]: Configures the transmission of tagged frames in a voice VLAN.

vlan-id: ID of the VLAN where the voice stream is transmitted. The value range is from 1 to 4094. This VLAN ID will be added to voice packets.

dot1p: Sets the VLAN ID in the VLAN tag to 0. This tag frame contains only the following priority information: *cos* and *dscp*.

cos *cos*: Configures the Class of Service (CoS) value for the voice stream in a voice VLAN. The value range is from 0 to 7, and the default value is **5**. A larger value indicates a higher priority. The CoS value is 0 for a common VLAN packet, indicating the lowest priority. By default, the CoS value of the voice stream packets transmitted to a voice VLAN is raised to 6, higher than the priority of a common VLAN packet. The CoS value indicates the L2 priority and is saved in the L2 header of a packet. It is filled in the **PRI** field of the IEEE 802.1Q VLAN tag.

dscp *dscp*: Configures the Differentiated Services Code Point (DSCP) for the voice stream in a voice VLAN. The value range is from 0 to 63, and the default value is **46**. A larger value indicates a higher priority. The DSCP value is 0 for a common IP packet, indicating the lowest priority. By default, the DSCP value of the voice stream packets transmitted to a voice VLAN is 46, higher than the priority of a common IP packet. The DSCP value indicates the IP priority (IP PRE) and is saved in the L3 header of a packet. For an IPv4 packet, the DSCP value is filled in the first six bits (bit 0 to bit 5) in the **ToS** field of the IPv4 packet header. For an IPv6 packet, the DSCP value is filled in the first six bits in the **Traffic Class** field of the IPv6 packet header.

untagged: Configures a VoIP device to transmit untagged frames. In this case, the VLAN ID and CoS value are ignored.

none: Indicates that no network policy is delivered, and the VoIP device determines the frames to be sent according to its configuration.

Command Modes

LLDP network-policy configuration mode

Default Level

14

Usage Guidelines

Configure an LLDP network policy after entering the LLDP network policy configuration mode.

If a device is connected to an IP phone in the downlink direction and the IP phone supports LLDP-MED, you can configure the Network Policy TLV to deliver a policy to the IP phone so that the IP phone changes the voice stream tag and QoS. The configuration procedure is as follows:

(1) Enable the voice VLAN function, and add the interface connected to the IP phone to the voice VLAN statically. For configuration details, see "Configuring Voice VLAN" in "Ethernet Switch."

(2) Configure the interface connected to the IP phone as an QoS trust interface (you are advised to use the DSCP trust mode). For configuration details, see "Configuring QoS" in "ACL and QoS."

(3) If 802.1x authentication is enabled on this interface, you also need to configure a secure channel to allow packets in the voice VLAN to pass. For details, see "Configuring ACL" in "ACL and QoS".

(4) If the IP phone does not support LLDP-MED, be sure to enable the voice VLAN function and add the MAC address of the IP phone to the voice VLAN OUI list manually.

Examples

The following example configures LLDP network policy 1, in which tagged frames need to be transmitted, the VLAN ID is set to 3, CoS is set to 4, and DSCP is set to 40.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp network-policy profile 1
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 dscp 40
Hostname(config-lldp-network-policy)# exit
```

The following example configures LLDP network policy 2, in which untagged frames need to be transmitted.

```
Hostname(config)# lldp network-policy profile 2
Hostname(config-lldp-network-policy)# voice vlan untagged
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **lldp enable**

IP Service Commands

1 ARP Commands

Command	Function
arp	Configure static Address Resolution Protocol (ARP) mapping entries.
arp-learning enable	Enable the ARP learning function.
arp anti-ip-attack	Configure the number of IP packets for triggering the discarding of ARP entries.
arp any-ip	Enable the any IP ARP function.
arp cache interface-limit	Set a limit on the number of ARP entries that can be learned by an interface.
arp fast-aging enable	Enable the fast ARP entry aging on an interface.
arp gratuitous-arp-learning enable	Enable the function of learning gratuitous ARP requests.
arp gratuitous-send interval	Enable the function of sending gratuitous ARP requests at intervals.
arp oob	Configure a static ARP entry for a management interface.
arp proxy-resolved	Configure the master VRRP device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as a proxy ARP.
arp rate-statistic enable	Enable the ARP packet rate statistics collection.
arp rate-statistic compute interval	Configure the interval for collecting ARP packet rate statistics.
arp resolve vlan	Configure ARP to actively send broadcast resolution requests to a specified sub VLAN in a super VLAN.
arp retry interval	Specify the ARP request retransmission interval.
arp retry times	Configure the number of times that an ARP request can be transmitted consecutively.
arp scan	Enable ARP scanning.
arp scan auto	Enable scheduled automatic ARP scanning.

arp scan interval	Configure the interval for scheduled automatic ARP scanning.
arp scan rate	Configure the rate of scheduled automatic ARP scanning.
arp suppress-auth-vlan-req	Restrain the device from sending ARP requests to authenticated VLANs.
arp switch-over resolve	Actively send ARP requests to terminals after active and standby VSU switchover.
arp timeout	Configure the timeout time for dynamic ARP entries in the ARP cache.
arp trusted	Configure the maximum number of trusted ARP entries.
arp trust-monitor enable	Enable ARP trust monitoring.
arp trusted aging	Enable trusted ARP aging.
arp trust user-vlan	Enable VLAN translation when a trusted ARP entry is added.
arp unresolve	Configure the maximum number of unresolved ARP entries.
arp strict-learning enable	Enable strict dynamic ARP learning.
arp filter gratuitous	Enable gratuitous ARP filtering.
arp filter acl	Enable ARP-based access control list (ACL) filtering.
arp filter smac-illegal	Enable the function of checking the source MAC addresses of ARP packets.
arp filter dmac-illegal	Enable the function of checking the destination MAC addresses of ARP packets.
arp warning-limit	Configure the ARP alarm rate limit.
clear arp-cache	Clear dynamic ARP mapping records in the ARP cache.
clear arp-cache trusted	Clear trusted ARP entries in the ARP cache.
clear arp-cache packet statistics	Clear ARP packet statistics.
ip proxy-arp	Enable proxy ARP on an interface.
local-proxy-arp	Enable local proxy ARP.
service trustedarp	Enable trusted ARP.

show arp	Display the ARP cache.
show arp oob	Display the ARP cache on a management interface.
show arp counter	Display the number of ARP entries in the ARP cache.
show arp detail	Display the details about the ARP cache.
show arp packet statistics	Display ARP packet statistics.
show arp rate-statistic	Display the ARP packet rate statistics.
show arp timeout	Display the aging time of dynamic ARP entries.
show arp flapping record	Display ARP flapping records.
show ip arp	Display the ARP cache.
show arp anti-attack statistics	Display the statistics on illegal ARP packets.

1.1 arp

Function

Run the **arp** command to configure static Address Resolution Protocol (ARP) mapping entries.

Run the **no** form of this command to remove this configuration.

No ARP static entry is configured by default.

Syntax

arp [**vrf** *vrf-name*] *ip-address mac-address arp-type*

no arp [**vrf** *vrf-name*] *ip-address*

Parameter Description

vrf *vrf-name*: Specifies a virtual routing and forwarding (VRF) instance. No VRF instance is specified by default. Static ARP entries are applied globally.

ip-address: IP address corresponding to a MAC address. The IP address is expressed in dotted decimal notation.

mac-address: Data link layer (DLL) address, consisting of 48 bits.

arp-type: ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Users can manually specify mappings between IP and MAC addresses to prevent the device from learning incorrect ARP entries.

After a static ARP entry is configured on a Layer 3 device, the device must learn the physical port corresponding to the MAC address in the entry before it performs Layer 3 routing.

Examples

The following example configures a static ARP entry for a host on the Ethernet by setting the IP address to 1.1.1.1 and the MAC address to 4e54.3800.0002.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

The following example configures a static ARP entry for a host on the Ethernet by setting the IP address to 1.1.1.1 and the MAC address to 4e54.3800.0002, and specifying a description of ABC.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa description ABC
```

Notifications

A VRF instance named xyz does not exist or the **address-family ipv4** command is not configured. When a static ARP entry is added to or deleted from the VRF instance, the following notification will be displayed:

```
% ARP:vrf xyz does not exist. Create first.
% ARP:vrf xyz ipv4 address-family is not enable. Enable first.
```

When a nonexistent static ARP entry or a reserved entry is deleted, the following notification will be displayed:

```
Cannot remove ARP. ARP entry does not exist or reserved.
```

When the ARP cache is fully occupied or the corresponding IP address is the local IP address, a static ARP entry fails to be added and the following notification will be displayed:

```
Cannot add static ARP.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp oob**
- **show arp**
- **show arp oob**
- **show arp counter**
- **show arp detail**

1.2 arp-learning enable

Function

Run the **arp-learning enable** command to enable the ARP learning function.

Run the **no** form of this command to disable this feature.

The ARP learning function is enabled by default.

Syntax

arp-learning enable

no arp-learning enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If this function is disabled on an interface, the interface does not learn dynamic ARP entries. Functions such as any IP ARP and authorized ARP detection will not take effect, either.

Examples

The following example disables the dynamic ARP learning function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no arp-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**
- **show arp counter**
- **show arp detail**

1.3 arp anti-ip-attack

Function

Run the **arp anti-ip-attack** command to configure the number of IP packets for triggering the discarding of ARP entries.

Run the **no** form of this command to restore the default configuration.

The default number of IP packets for triggering the discarding of ARP entries is 3.

Syntax

arp anti-ip-attack *attack-num*

no arp anti-ip-attack

Parameter Description

attack-num: Number of IP packets for triggering the discarding of ARP entries. The value range is from 0 to 100, and the default value is **3**. The value **0** indicates that ARP-based IP guard is disabled.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When receiving unresolved IP packets, the device sends them to the CPU for address resolution, that is, ARP learning, instead of forwarding them through the hardware. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting services on the device.

After ARP-based IP guard is enabled, the device will count the number of received ARP packets based on the destination IP address. When the number of packets with the same destination IP address exceeds a certain threshold, the device deems it as a CPU attack and will send a drop entry to the hardware. Then the hardware will not send subsequent ARP packets with this destination IP address to the CPU. After the address resolution is complete, the device updates the entry to the forwarding state and continues to forward the packets with this destination IP address.

This function requires routing resources on the device hardware. Therefore, if hardware resources are sufficient, set *attack-num* to a smaller value. If hardware resources are insufficient, set *attack-num* to a larger value or disable this function.

Examples

The following example sets the number of IP packets for triggering the discarding of ARP entries to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp anti-ip-attack 5
```

The following example disables ARP-based IP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp anti-ip-attack 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.4 arp any-ip

Function

Run the **arp any-ip** command to enable the any IP ARP function.

Run the **no** form of this command to disable this feature.

The any IP ARP function is disabled by default.

Syntax

arp any-ip

no arp any-ip

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The any IP ARP function allows users to access the Internet with any IP address. This applies when a user uses a laptop in a hotel and wants to access the Internet without changing the configured IP address and gateway.

This function is not applicable in the following two scenarios, in which a user must modify the configuration before the user can access the Internet.

- The user's IP address is on the same network segment as the interface directly connected to the device. However, the configured gateway IP address is not the IP address configured for the interface directly connected to the device.
- The user's IP address is not on the same network segment as the interface directly connected to the device, but on the network segment of another interface. That means an IP address conflict occurs.

  As the user's IP address is not on the same network segment as the interface directly connected to the device, the dynamic ARP entry and direct route are generated only when the user initiates an ARP request. Therefore, in some scenarios (including but not limited to the following ones), the user will not be able to access the Internet unless the ARP entry is cleared and the gateway address is relearned on the user host.

  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, the administrator deletes the dynamic ARP entry from the device. As a result, the user's dynamic ARP entry and direct route are removed and the user cannot receive the reply packet.
  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, any IP ARP is disabled and then enabled again on the interface. When the any IP ARP function is disabled on the interface, the user's dynamic ARP entries and direct routes are immediately deleted. As a result, the user cannot receive the reply.

Caution

If static ARP entries or the ARP entries involving the Virtual Router Redundancy Protocol (VRRP) IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, and any IP ARP does not take effect.

Examples

The following example enables any IP ARP on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp any-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**
- **show arp counter**
- **show arp detail**

1.5 arp cache interface-limit

Function

Run the **arp cache interface-limit** command to set a limit on the number of ARP entries that can be learned by an interface.

Run the **no** form of this command to restore the default configuration.

No limit is set for the number of ARP entries that can be learned by an interface by default.

Syntax

arp cache interface-limit *limit*

no arp cache interface-limit

Parameter Description

limit: Maximum number of ARP entries that can be learned by an interface, including static ARP entries and dynamic ARP entries. The value range is from 0 to 16000. The default value is **0**, indicating no limit on the number of ARP entries that can be learned by an interface.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Limiting the number of ARP entries that can be learned by an interface can protect the device against malicious ARP attacks that can result in excessive ARP entries and CPU resource consumption. The configured *limit* value must be equal to or greater than the number of the ARP entries that have been learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Examples

The following example sets the limit on the number of ARP entries that can be learned by port GigabitEthernet 0/1 to 300.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp cache interface-limit 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**

1.6 arp fast-aging enable

Function

Run the **arp fast-aging enable** command to enable the fast ARP entry aging on an interface.

Run the **no** form of this command to restore the default configuration.

The fast ARP entry aging function is disabled by default.

Syntax

arp fast-aging enable

no arp fast-aging enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Dynamic ARP entries start aging one hour after the aging of their corresponding MAC addresses. If this feature is configured, after their corresponding MAC address age, the dynamic ARP entries age immediately. Pay attention to the following points:

- This command can be configured only on switch virtual interfaces (SVIs).
- When the conversion of ARP entries into host routes is enabled on the device, you are advised to enable this function at the same time, to help achieve fast route convergence.

Examples

The following example enables fast ARP entry aging on interface VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp fast-aging enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp timeout**

1.7 arp gratuitous-arp-learning enable

Function

Run the **arp gratuitous-arp-learning enable** command to enable the function of learning gratuitous ARP requests.

Run the **no** form of this command to disable this feature.

The function of learning gratuitous ARP requests is enabled by default.

Syntax

arp gratuitous-arp-learning enable

no arp gratuitous-arp-learning enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example disables the function of learning gratuitous ARP requests.

```
Hostname> enable
Hostname# configure terminalHostname(config-if-VLAN 1)# no arp
gratuitous-arp-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp gratuitous-send interval**

1.8 arp gratuitous-send interval

Function

Run the **arp gratuitous-send interval** command to enable the function of sending gratuitous ARP requests at intervals.

Run the **no** form of this command to disable this feature.

The function of sending gratuitous ARP requests at intervals is disabled by default.

Syntax

arp gratuitous-send interval *interval* [*number*]

no arp gratuitous-send

Parameter Description

interval: Interval for sending gratuitous ARP requests, in seconds. The value range is from 1 to 3600.

number: Number of gratuitous ARP requests to be sent. The value range is from 1 to 100, and the default value is **1**.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When a network interface of a device acts as the gateway of downlink devices, if a downlink device pretends to be the gateway, you can enable the function of sending gratuitous ARP requests at intervals on the interface to advertise the MAC address of the real gateway.

Examples

The following example sends a gratuitous ARP request to interface VLAN 1 every second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp gratuitous-send interval 1 1
```

The following example disables the function of sending gratuitous ARP requests to interface VLAN 1 at intervals.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no arp gratuitous-send
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp gratuitous-arp-learning enable**

1.9 arp oob

Function

Run the **arp oob** command to configure a static ARP entry for a management interface.

Run the **no** form of this command to remove this configuration.

No static ARP entry of any management interface is configured in the ARP cache by default.

Syntax

arp oob [*mgmt-name*] *ip-address mac-address arp-type*

no arp oob [*mgmt-name*] *ip-address*

Parameter Description

mgmt-name: Management interface bound to a static ARP entry when multiple management interfaces are supported. The first management interface of a device is bound when *mgmt-name* is not specified.

ip-address: IP address corresponding to a MAC address. The IP address is expressed in dotted decimal notation.

mac-address: DLL address, consisting of 48 bits.

arp-type: ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example configures a static ARP entry for the host management interface on the Ethernet. The IP address is set to 1.1.1.1 and the MAC address is set to 4e54.3800.0002.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa
```

Notifications

When the ARP cache is fully occupied or the corresponding IP address is the local IP address, a static ARP entry fails to be added and the following notification will be displayed:

```
Cannot add static ARP.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp oob**

1.10 arp proxy-resolved

Function

Run the **arp proxy-resolved** command to configure the master VRRP device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as a proxy ARP.

Run the **no** form of this command to remove this configuration.

By default, the master VRRP device judges the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as a proxy ARP.

Syntax

arp proxy-resolved

no arp proxy-resolved

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After the **arp proxy-resolved** command is configured, the master VRRP device, upon receiving an ARP request, first judges whether the ARP entry corresponding to the destination IP address exists. If yes, the master VRRP device acts as a proxy ARP to give a reply. If no, the master VRRP device does not act as a proxy ARP. In addition, the gateway automatically broadcasts the ARP request for the destination IP address. This prevents the case that the gateway fails to act as a proxy to respond to an ARP request of the destination IP address due to absence of the ARP entry corresponding to the destination IP address.

After the **no arp proxy-resolved** command is configured, if the proxy conditions are met, the master VRRP device directly acts as a proxy upon receiving an ARP request, without judging whether the ARP entry corresponding to the destination IP address has been resolved.

Examples

The following example configures the master VRRP device not to judge the existence of the ARP entry corresponding to a destination IP address when the device acts as a proxy ARP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no arp proxy-resolved
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 arp rate-statistic enable

Function

Run the **arp rate-statistic enable** command to enable the ARP packet rate statistics collection.

Run the **no** form of this command to disable this feature.

The ARP packet rate statistics collection is disabled by default.

Syntax

arp rate-statistic enable

no arp rate-statistic enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example enables the ARP packet rate statistics collection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp rate-statistic enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp rate-statistic**

1.12 arp rate-statistic compute interval

Function

Run the **arp rate-statistic compute interval** command to configure the interval for collecting ARP packet rate statistics.

Run the **no** form of this command to remove this configuration.

The default interval for collecting ARP packet rate statistics is 5 seconds.

Syntax

arp rate-statistic compute interval *interval*

no arp rate-statistic compute interval

Parameter Description

interval: Sampling interval, in seconds. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example sets the interval for collecting ARP packet rate statistics to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp rate-statistic compute interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp rate-statistic**
- **arp rate-statistic enable**

1.13 arp resolve vlan

Function

Run the **arp resolve vlan** command to configure ARP to actively send broadcast resolution requests to a specified sub VLAN in a super VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

ARP does not actively send broadcast resolution requests to a specified sub VLAN in a super VLAN by default.

Syntax

arp resolve vlan { *vlan-list* | **none** }

no arp resolve vlan { *vlan-list* | **none** }

default arp resolve vlan

Parameter Description

vlan-list: Sub VLAN segment. When ARP is configured to actively send broadcast resolution requests to VLANs in the sub VLAN segments in a super VLAN, ARP will only send ARP broadcast packets to these VLANs. The start and end VLANs in a sub VLAN segment are connected by a hyphen (-), and multiple sub VLAN segments are separated by commas (,), for example, 1, 3-5.

none: Indicates that no ARP broadcast requests will be sent to any sub VLAN in a super VLAN.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

In a super VLAN scenario, when the device actively sends ARP resolution requests, the ARP resolution requests are broadcast to the entire super VLAN by default. If there are many sub VLANs in the super VLAN, the packets will be replicated in large quantities, which will affect the performance of the device.

Most terminals (such as PCs or servers) request ARP information of the gateway before accessing the network. Therefore, there is no need to actively broadcast the ARP resolution requests to the sub VLANs where these terminals reside. For dumb terminals that do not actively send gratuitous ARP packets, this command can be deployed in a specified *vlan-list* to enable the device to actively send ARP resolution requests to these VLANs.

Caution

After the **arp resolve vlan** *vlan-list* command is run, the device will only send ARP broadcast requests to the VLANs specified in *vlan-list* in the super VLAN, and other sub VLANs not in *vlan-list* will not receive ARP broadcast requests. In particular, if an authentication-exempt VLAN is configured and the authentication-exempt VLAN is not in *vlan-list* of **arp resolve vlan**, ARP requests will not be broadcast to the authentication-exempt VLAN.

Examples

The following example configures ARP to actively send broadcast resolution requests to sub VLANs 0-20 and 25-30 in the super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp resolve vlan 10-20,25-30
```

The following example cancels sending resolution requests to VLANs 10-20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no arp resolve vlan 10-20
```

The following example configures the device not to actively send ARP resolution requests to any sub VLAN in the super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp resolve vlan none
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 arp retry interval

Function

Run the **arp retry interval** command to specify the ARP request retransmission interval.

Run the **no** form of this command to restore the default configuration.

The default ARP request retransmission interval is 1 second.

Syntax

arp retry interval *interval*

no arp retry interval

Parameter Description

interval: ARP request retransmission interval, in seconds. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

The ARP request retransmission interval can be configured globally and on a Layer 3 interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the ARP request retransmission interval is set to 5 seconds in global configuration mode and set to 2 seconds on SVI 1, the ARP request retransmission interval of SVI 1 is 2 seconds. The ARP request retransmission interval of other interfaces (including new interfaces) is subject to global configuration, that is, 5 seconds.

The shorter the retransmission interval is, the faster the resolution is, and the more bandwidth will be consumed. If the network resources are insufficient, you are advised to set the ARP request retransmission interval to a larger value to reduce the consumption of network bandwidths. Generally, the interval should not be greater than the aging time of dynamic ARP entries.

Examples

The following example sets the ARP request retransmission interval to 30 seconds in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp retry interval 30
```

The following example sets the ARP request retransmission interval of SVI 1 to 18 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp retry interval 18
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp retry times**

1.15 arp retry times

Function

Run the **arp retry times** command to configure the number of times that an ARP request can be transmitted consecutively.

Run the **no** form of this command to restore the default configuration.

The default number of times that an ARP request can be transmitted consecutively is 5. That is, if no ARP reply packet is received, the device sends the ARP request packets for another four times.

Syntax

arp retry times *times*

no arp retry times

Parameter Description

times: Number of times that the same ARP request can be transmitted. The value range is from 1 to 100, and the default value is **5**. When the value is set to **1**, an ARP request is sent once, and will not be retransmitted.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

The number of times that an ARP request can be transmitted consecutively can be configured globally and on a Layer 3 interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the number of times that an ARP request can be transmitted consecutively is set to 1 in global configuration mode and set to 3 on SVI 1, the number of times that an ARP request can be transmitted is 3 for SVI 1. The number of times that an ARP request can be transmitted on other interfaces (including new interfaces) is subject to global configuration, that is, 1.

The more times an ARP packet can be transmitted consecutively, the more likely the resolution will succeed, and the more bandwidth will be consumed. If the network resources are insufficient, you are advised to set the number of times to a smaller value to reduce the consumption of network bandwidths.

Examples

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 1 in global configuration mode, that is, ARP request packets will not be retransmitted.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp retry times 1
```

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 2 in global configuration mode, that is, an ARP request packet will be retransmitted once.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# arp retry times 2
```

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 5 for SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp retry times 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp retry interval**

1.16 arp scan

Function

Run the **arp scan** command to enable ARP scanning.

Run the **no** form of this command to disable this feature.

ARP scanning is disabled by default.

Syntax

arp scan [*start-ip-address end-ip-address*]

no arp scan [*start-ip-address end-ip-address*]

Parameter Description

start-ip-address: Start IP address of the ARP scanning range. The start IP address must be smaller than or equal to the end IP address.

end-ip-address: End IP address of the ARP scanning range. The end IP address must be greater than or equal to the start IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

This function is usually used together with the Web-based dynamic-to-static ARP entry conversion function.

By configuring the IP address range for ARP scanning, users can scan neighbors in this range, thereby reducing the waiting time. The number of hosts in the ARP scanning range must not exceed 1,024.

The start and end IP addresses of the ARP scanning range must be on the same network segment as the interface IP address that may serve as the master or slave IP address.

If the start and end IP addresses are not specified, only the neighbors on the same network segment as the master IP address of the interface are scanned. The subnet mask of the master IP address must consist of at least 22 bits.

ARP scanning configuration takes effect only once. It cannot be saved and will lose effect the next time. ARP scanning takes effect when the Layer 3 interface is up (that is, the link is up and an IP address is configured).

Examples

The following example enables ARP scanning on port GigabitEthernet 0/1 without specifying the IP address range.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp scan
```

The following example enables ARP scanning on port GigabitEthernet 0/0 with the IP address range specified.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/0
Hostname(config-if-GigabitEthernet 0/0)# arp scan 1.1.1.1 1.1.1.10
```

Notifications

When a start IP address or end IP address is not a valid host address, or the start IP address is greater than the end IP address, or the start IP address and end IP address are not on the same network segment as the interface IP address, the following notification will be displayed:

```
%notice: Invalid ip address range.
```

When the number of hosts in a specified range is greater than 1,024, the following notification will be displayed:

```
%notice: Failed to scan because ip address range is larger than 1024.
```

When no Layer 3 interface is up, the following notification will be displayed:

```
%notice: Failed to scan because this interface is not up.
```

Common Errors

- The start IP address is greater than the end IP address.
- The start IP address and the end IP address are not on the same network segment as the IP interface address.

Platform Description

This command is supported only on egress gateways (EGs), network provider edges (NPEs), and network border routers (NBRs).

Related Commands

- **arp scan auto**

1.17 arp scan auto

Function

Run the **arp scan auto** command to enable scheduled automatic ARP scanning.

Run the **no** form of this command to disable this feature.

The scheduled automatic ARP scanning function is disabled by default.

Syntax

arp scan auto [*start-ip-address end-ip-address*]

no arp scan auto [*start-ip-address end-ip-address*]

Parameter Description

start-ip-address: Start IP address of the ARP scanning range. The start IP address must be smaller than or equal to the end IP address.

end-ip-address: End IP address of the ARP scanning range. The end IP address must be greater than or equal to the start IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The scheduled automatic ARP scanning function is enabled by default, and scheduled automatic ARP scanning is performed once every 5 minutes. It takes effect only on interfaces in the up state.

By configuring the IP address range for ARP scanning, users can scan neighbors in this range, thereby reducing the waiting time. The number of hosts in the ARP scanning range must not exceed 1,024.

The IP addresses of neighbors with ARP entries available will not be scanned.

Up to 30 instances can be configured.

Examples

The following example enables scheduled automatic ARP scanning on VLAN 1, with the IP address range from 1.1.1.1 to 1.1.1.10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp scan auto 1.1.1.1 1.1.1.10
```

Notifications

When a start IP address or end IP address is not a valid host address, or the start IP address is greater than the end IP address, the following notification will be displayed:

```
Invalid ip address range.
```

When the number of hosts in a specified range is greater than 1,024, the following notification will be displayed:

```
Failed to scan because ip address range is larger than 1024.
```

When more than 30 instances are configured, the following notification will be displayed:

```
The number of arp auto-scan ip exceed 30.
```

Common Errors

- The start IP address is greater than the end IP address.
- The number of hosts in a specified range is greater than 1,024.

Platform Description

N/A

Related Commands

- **arp scan**
- **arp scan interval**
- **arp scan rate**

1.18 arp scan interval

Function

Run the **arp scan interval** command to configure the interval for scheduled automatic ARP scanning.

Run the **no** form of this command to restore the default configuration.

The default interval of scheduled automatic ARP scanning is 5 minutes.

Syntax

arp scan interval *time*

no arp scan interval

Parameter Description

time: Interval of scheduled ARP scanning, in minutes. The range is from 1 to 30.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

The interval is the duration between the end of scanning on all interfaces and the start of the next scanning.

Examples

The following example sets the interval of scheduled ARP scanning to 1 minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp scan interval 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp scan auto**
- **arp scan rate**

1.19 arp scan rate

Function

Run the **arp scan rate** command to configure the rate of scheduled automatic ARP scanning.

Run the **no** form of this command to remove this configuration.

The default scheduled automatic ARP scanning rate is **20** IP addresses per second.

Syntax

arp scan rate *rate-value*

no arp scan rate

Parameter Description

rate-value: Rate of scheduled automatic ARP scanning, in IP addresses per second. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

The scanning rate is the number of IP addresses that the device scans and successfully learns the ARP packets from per second. For example, when the rate is set to 100, the device scans a maximum of 100 IP addresses per second.

If scanning has be done on all the required network segments and ARP packets have been successfully learned, the next scanning rate is 0.

Examples

The following example sets the rate of scheduled automatic ARP scanning to 8 0 IP addresses per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp scan rate 80
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp scan auto**
- **arp scan interval**

1.20 arp suppress-auth-vlan-req

Function

Run the **arp suppress-auth-vlan-req** command to restrain the device from sending ARP requests to authenticated VLANs.

Run the **no** form of this command to remove this configuration.

ARP requests are not sent to authenticated VLANs by default.

Syntax

arp suppress-auth-vlan-req

no arp suppress-auth-vlan-req

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

This configuration is supported only on SVIs.

In gateway authentication mode, all sub VLANs in a super VLAN are authenticated VLANs by default. Users in an authenticated VLAN have to pass authentication before accessing the network. After authentication, a static ARP entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send ARP requests to the authenticated VLAN. If the device attempts to access users in an authentication-exempt VLAN, it only needs to send ARP requests to the authentication-exempt VLAN.

In gateway authentication mode, the device does not send ARP requests to authenticated VLANs by default. If the device needs to access authentication-exempt users in an authenticated VLAN, disable this function.

Examples

The following example enables the function of sending ARP requests to authenticated VLANs on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no arp suppress-auth-vlan-req
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 arp switch-over resolve

Function

Run the **arp switch-over resolve** command to actively send ARP requests to terminals after active and standby VSU switchover.

Run the **no** form of this command to remove this configuration.

ARP requests are not actively sent to terminals after active and standby VSU switchover by default.

Syntax

arp switch-over resolve

no arp switch-over resolve

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

This function can be enabled to quickly update ARP entries of a downlink device after active and standby VSU switchover, especially when the downlink device is similar to a server with dual network interface cards. When the slave device becomes the master, it will actively send ARP requests to SVIs (instead of interfaces not in a super VLAN) of up to 1000 downlink terminals to trigger the terminals to reply to these ARP requests. Then, the device can update the ARP and MAC tables.

Examples

The following example actively sends ARP requests to terminals after active and standby VSU switchover.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp switch-over resolve
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 arp timeout

Function

Run the **arp timeout** command to configure the timeout time for dynamic ARP entries in the ARP cache.

Run the **no** form of this command to restore the default configuration.

The default timeout time of dynamic ARP entries in the ARP cache is **3600** seconds.

Syntax

arp timeout *time*

no arp timeout

Parameter Description

time: Timeout time, in seconds. The value range is from 0 to 2147483.

Command Modes

Interface configuration mode

Global configuration mode

Default Level

2

Usage Guidelines

The ARP timeout configuration only applies to the dynamic mappings between IP and MAC addresses. When the ARP timeout time is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, the ARP timeout time does not need to be configured.

The ARP aging time can be configured globally and on a specified interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the ARP aging time is set to 3,000 seconds in global configuration mode and to 1,800 seconds on interface 1, the ARP aging time of interface 1 is 1800s. The ARP aging time of other interfaces (including new interfaces) is subject to the global ARP aging time, that is, 3,000s.

Examples

The following example sets the timeout time of dynamic ARP entries learned by port GigabitEthernet 0/1 to 120s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp timeout 120
```

The following example sets the ARP aging time to 3,000 seconds globally. If no aging time is configured for an interface, the ARP aging time is 3000 seconds for all Layer 3 interfaces.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp timeout 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp timeout**

1.23 arp trusted

Function

Run the **arp trusted** command to configure the maximum number of trusted ARP entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of trusted ARP entries is **8000** by default.

Syntax

arp trusted *number*

no arp trusted

Parameter Description

number: Maximum number of trusted ARP entries. The value range is from 10 to 14976.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Enable trusted ARP before configuring this function. Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the number based on the actual requirement. Do not set it to an excessively large value.

The maximum value of the *number* parameter can be the capacity of the ARP table minus 1,024.

Examples

The following example sets the maximum number of trusted ARP entries to 1,000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trusted 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **service trustedarp**

1.24 arp trust-monitor enable

Function

Run the **arp trust-monitor enable** command to enable ARP trust monitoring.

Run the **no** form of this command to disable this feature.

ARP trust monitoring is disabled by default.

Syntax

arp trust-monitor enable

no arp trust-monitor enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

ARP trust monitoring is used to prevent excessive useless ARP entries generated due to ARP spoofing from occupying device resources. After ARP trust monitoring is enabled on a Layer 3 interface and the device receives an ARP request from this interface:

(1) If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs neighbor unreachability detection (NUD) after 1 to 5 seconds. That is, the device ages the newly learned ARP entry and unicasts an ARP request. If the device receives an ARP update packet from the peer within the aging time, it stores the entry. Otherwise, it deletes the entry.

(2) If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD.

(3) If the MAC address in the existing dynamic ARP entry is updated, the device performs NUD.

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Examples

The following example enables ARP trust detection on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp trust-monitor enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 arp trusted aging

Function

Run the **arp trusted aging** command to enable trusted ARP aging.

Run the **no** form of this command to restore the default configuration.

Trusted ARP entries are not aged by default.

Syntax

arp trusted aging

no arp trusted aging

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Trusted ARP aging can be configured, with the aging time same as the dynamic ARP aging time. You can run the **arp timeout** command in interface configuration mode to configure the aging time.

Examples

The following example enables trusted ARP aging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trusted aging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp timeout**

1.26 arp trust user-vlan

Function

Run the **arp trust user-vlan** command to enable VLAN translation when a trusted ARP entry is added.

Run the **no** form of this command to remove this configuration.

The VLAN translation is disabled when a trusted ARP entry is added by default.

Syntax

arp trust user-vlan *vlan-id* **translated-vlan** *vlan-id*

no arp trust user-vlan *vlan-id* **translated-vlan** *vlan-id*

Parameter Description

user-vlan *vlan-id*: Indicates the VLAN ID set for a server.

translated-vlan *vlan-id*: Indicated the VLAN ID after translation.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Enable trusted APR before configuring this function.

Configure this command only when the VLAN delivered by the server differs from the valid VLAN in the trusted ARP entry.

Examples

The following example enables VLAN translation when a trusted ARP entry is added. A server delivers VLAN 3 but actually, trusted ARP takes effect on VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trust user-vlan 3 translated-vlan 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 arp unresolve

Function

Run the **arp unresolve** command to configure the maximum number of unresolved ARP entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of unresolved ARP entries that can be held in an ARP cache is **16000** by default.

Syntax

arp unresolve *unresolved-number*

no arp unresolve

Parameter Description

unresolved-number: Maximum number of unresolved ARP entries. The value range is from 1 to 16000.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

In a local area network (LAN), ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the hosts. To prevent this situation, if a large number of unresolved entries exist in the ARP cache and remain in the cache after a while, you are advised to use this command to limit the number of unresolved ARP entries.

Examples

The following example sets the maximum number of unresolved ARP entries on the device to 500.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp unresolve 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

-
-

-

1.28 arp strict-learning enable

Function

Run the **arp strict-learning enable** command to enable strict dynamic ARP learning.

Run the **no** form of this command to disable this feature.

Strict dynamic ARP learning is disabled by default.

Syntax

arp strict-learning enable

no arp strict-learning enable

Parameter Description

N/A

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

After strict dynamic ARP learning is enabled, only the reply packets in response to the ARP request packets actively sent by the device can trigger the device to learn ARP entries.

The strict dynamic ARP learning can be configured globally and on an interface. The configuration in interface configuration mode takes priority over that in global configuration mode.

Examples

The following example enables strict dynamic ARP learning globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp strict-learning enable
```

The following example disables strict dynamic ARP learning globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no arp strict-learning enable
```

The following example enables strict dynamic ARP learning on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/10)# arp strict-learning enable
```

The following example disables strict dynamic ARP learning on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no arp strict-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.29 arp filter gratuitous

Function

Run the **arp filter gratuitous** command to enable gratuitous ARP filtering.

Run the **no** form of this command to disable this feature.

Gratuitous ARP filtering is disabled by default.

Syntax

arp filter gratuitous

no arp filter gratuitous

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example enables gratuitous ARP filtering.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter gratuitous
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.30 arp filter acl

Function

Run the **arp filter acl** command to enable ARP-based access control list (ACL) filtering.

Run the **no** form of this command to disable this feature.

ARP-based ACL filtering is disabled by default.

Syntax

arp filter acl *acl-number*

no arp filter acl

Parameter Description

acl-number: Associated ACL. The value range is from 1 to 199 and 1300 to 2899.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets that hit ACL rules.

Examples

The following example enables ARP-based ACL filtering.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter acl 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.31 arp filter smac-illegal

Function

Run the **arp filter smac-illegal** command to enable the function of checking the source MAC addresses of ARP packets.

Run the **no** form of this command to disable this feature.

The function of checking the source MAC addresses of ARP packets is disabled by default.

Syntax

arp filter smac-illegal

no arp filter smac-illegal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets whose source MAC addresses is not consistent with the Ethernet source MAC address.

Examples

The following example enables the function of checking the source MAC addresses of ARP packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter smac-illegal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.32 arp filter dmac-illegal

Function

Run the **arp filter dmac-illegal** command to enable the function of checking the destination MAC addresses of ARP packets.

Run the **no** form of this command to disable this feature.

The function of checking the destination MAC addresses of ARP packets is disabled by default.

Syntax

arp filter dmac-illegal

no arp filter dmac-illegal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets whose destination MAC addresses is not consistent with the Ethernet destination MAC address.

Examples

The following example enables the function of checking the destination MAC addresses of ARP packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter dmac-illegal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show arp anti-attack statistics
-

1.33 arp warning-limit

Function

Run the **arp warning-limit** command to configure the ARP alarm rate limit.

Run the **no** form of this command to restore the default configuration.

The default ARP alarm rate limit interval is 50 seconds and the default upper limit of alarms allowed within this interval is 10.

Syntax

arp warning-limit interval *interval* **times** *time*

no arp warning-limit

Parameter Description

interval *interval*: Specifies the ARP alarm rate limit interval, in seconds. The value range is 1 to 180. The default value is **50**.

times *time*: Specifies the upper limit of alarms allowed within the ARP alarm rate limit interval. The value range is from 1 to 1,024, and the default value is **10**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

This command can be used to adjust the printing rate of ARP syslog alarms. The actual ARP alarm rate may be lower than the configured rate, depending on system performance.

Examples

The following example sets the ARP alarm rate limit interval to 60 seconds and the upper limit of alarms allowed within this interval to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp warning-limit interval 60 times 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

This is applicable to devices with multiple line cards.

Related Commands

N/A

1.34 clear arp-cache

Function

Run the **clear arp-cache** command to clear dynamic ARP mapping records in the ARP cache.

Syntax

clear arp-cache [[**vrf** *vrf-name* | **oob**] [*ip-address* [*mask*]] | [**interface** *interface-type interface-number*]]

Parameter Description

vrf *vrf-name*: Deletes dynamic ARP entries of a specified VRF instance. If this parameter is not specified, it indicates the public network instance.

oob: Configures out-of-band management.

ip-address: IP address whose dynamic ARP entries are to be deleted. All dynamic ARP entries are deleted by default.

mask: Subnet mask. After this parameter is specified, dynamic ARP entries in the subnet will be deleted and the preceding IP address must be set to a subnet ID. Dynamic ARP entries specified in the *ip-address* parameter are deleted by default.

interface *interface-type interface-number*: Clears the dynamic ARP entries of a specified interface. Dynamic ARP entries of all interfaces are deleted by default.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

In gateway authentication mode, dynamic ARP entries in authenticated VLANs will not be cleared.

On devices enabled with the Network Foundation Protection Policy (NFPP), only one ARP packet is received for each MAC address (or IP address) per second by default. If the **clear arp-cache** command is run twice within 1 second, the second reply may be filtered out and the ARP resolution may fail.

Examples

The following example clears all dynamic ARP entries in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache
```

The following example clears dynamic entry 1.1.1.1 in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache 1.1.1.1
```

The following example deletes dynamic ARP entries of SVI 1.

```
Hostname> enable
Hostname# clear arp-cache interface Vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 clear arp-cache trusted

Function

Run the **clear arp-cache trusted** command to clear trusted ARP entries in the ARP cache.

Syntax

clear arp-cache [**vrf** *vrf-name* | **oob**] **trusted** [*ip-address* [*mask*]]

Parameter Description

vrf *vrf-name*: Deletes dynamic ARP entries of a specified VRF instance. If this parameter is not specified, it indicates the public network instance.

oob: Configures out-of-band management.

ip-address: IP address whose trusted ARP entries are to be deleted. All trusted ARP entries are deleted by default.

mask: Subnet mask. After this parameter is specified, trusted ARP entries in the subnet will be deleted and the preceding IP address must be set to a subnet ID. Trusted ARP entries specified in the *ip-address* parameter are deleted by default.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example clears all trusted ARP entries in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache trusted
```

The following example clears trusted ARP entries with the IP address of 1.1.1.1 in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache trusted 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 clear arp-cache packet statistics

Function

Run the **clear arp-cache packet statistics** command to clear ARP packet statistics.

Syntax

clear arp-cache packet statistics [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

After ARP packet statistics are cleared, packet statistic starts from 0 again.

Examples

The following example clears ARP packet statistics.

```
Hostname> enable
Hostname# clear arp-cache packet statistics
```

The following example clears ARP packet statistics on VLAN 1.

```
Hostname> enable
Hostname# clear arp-cache packet statistics vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp packet statistics**

1.37 ip proxy-arp

Function

Run the **ip proxy-arp** command to enable proxy ARP on an interface.

Run the **no** form of this command to disable this feature.

Proxy ARP is disabled by default.

Syntax

ip proxy-arp

no ip proxy-arp

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The device enabled with proxy ARP can help a host obtain MAC addresses of IP hosts in other networks or subnets. When a proxy device receives an ARP request whose sender's source IP address is in a different network from the destination IP address, if the device knows the route to the destination IP address, it sends an ARP reply containing its own Ethernet MAC address.

By default, proxy ARP is disabled on Layer 3 devices.

Examples

The following example enables proxy ARP on port GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip proxy-arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface** (IP service information/IPv4 basic information)

1.38 local-proxy-arp

Function

Run the **local-proxy-arp** command to enable local proxy ARP.

Run the **no** form of this command to disable this feature.

Local proxy ARP is disabled by default.

Syntax

local-proxy-arp

no local-proxy-arp

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

After local proxy ARP is enabled, the device can help hosts obtain the MAC addresses of other hosts in the same subnet. For example, when port protection is enabled on the device, users connected to different ports of the device are isolated at Layer 2. After local proxy ARP is enabled and the device receives an ARP request, the device acts as a proxy and sends an ARP reply containing its own Ethernet MAC address. In this case, different users communicate with each other through Layer 3 routes.

Examples

The following example enables local proxy ARP in VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# local-proxy-arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface** (IP service information/IPv4 basic information)

1.39 service trustedarp

Function

Run the **service trustedarp** command to enable trusted ARP.

Run the **no** form of this command to disable this feature.

Trusted ARP is disabled by default.

Syntax

service trustedarp

no service trustedarp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When a user goes online on a GPRS support node (GSN) client, the authentication server obtains the user's real mapping between IP and MAC addresses through the access switch, and adds trusted ARP entries on the user's gateway switch. This process is transparent to the network administrator and does not require extra work from them.

Trusted ARP entries have characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries and lower than that of static ARP entries. Trusted ARP entries have an aging mechanism similar to that of dynamic ARP entries. Before an ARP entry ages, the device actively sends an ARP request to detect whether the corresponding host exists. If the host sends a reply, the device regards the host

active and updates the aging time of the ARP entry. Otherwise, the device deletes the ARP entry. Trusted ARP entries have characteristics of static ARP entries. The device will not dynamically update the MAC addresses and interfaces in the trusted ARP entries by learning ARP packets.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeting the gateway.

Examples

The following example enables trusted ARP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service trustedarp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp trusted**
- **arp trusted aging**
- **arp trust user-vlan**

1.40 show arp

Function

Run the **show arp** command to display the ARP cache.

Syntax

show arp [*interface-type interface-number* | **trusted** [*ip-address* [*mask*]] | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **complete** | **incomplete** | **static**]

Parameter Description

interface-type interface-number: *interface-type* indicates the interface type and *interface-number* indicates the interface number. After the parameter is specified, the ARP entries of a specified Layer 3 interface or Layer 2 interface are displayed.

vrf *vrf-name*: Displays the ARP entries of a specified VRF instance.

trusted: Displays trusted ARP entries. Currently, only the global VRF instance supports trusted ARP entries.

ip-address: IP address whose ARP entries need to be displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.

mask: Subnet mask. After this parameter is specified, ARP entries within the IP subnet will be displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.

mac-address: MAC address whose ARP entries need to be displayed.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

static: Displays all static ARP entries and their sources.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache.

```
Hostname> enable
Hostname# show arp
Total Numbers of Arp: 7
Protocol  Address         Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   0        0013.20a5.7a5f  arpa   VLAN 1
Internet  192.168.195.67   0        001a.a0b5.378d  arpa   VLAN 1
Internet  192.168.195.65   0        0018.8b7b.713e  arpa   VLAN 1
Internet  192.168.195.64   0        0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.63   0        001a.a0b5.3990  arpa   VLAN 1
Internet  192.168.195.62   0        001a.a0b5.0b25  arpa   VLAN 1
Internet  192.168.195.5    --       00d0.f822.33b1  arpa   VLAN 1
```

The following example displays the ARP entry of IP address 192.168.195.68.

```
Hostname> enable
Hostname# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

The following example displays ARP entries of IP subnet 92.168.195.0/24.

```
Hostname> enable
Hostname# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5    --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

The following example displays the ARP entry of MAC address 001a.a0b5.378d.

```
Hostname> enable
Hostname# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

The following example displays all static ARP entries and their sources.

```
Hostname> enable
Hostname# show arp static
Protocol  Address  Age(min)  Hardware  Type   Interface        Origin
Internet  192.168.23.55    <static>  0000.0000.0010  arpa   VLAN 100   Configure
Internet  192.168.23.56    <static>  0000.0000.0020  arpa   VLAN 100
Authentication
Internet  192.168.23.57    <static>  0000.0000.0020  arpa   VLAN 100   DHCP-Snooping
2  static arp entries exist.
```

Table 1-1 Output Fields of the show arp Command

Field	Description
Protocol	Protocol. **Internet** indicates the Internet protocol.
Address	IPv4 address.
Age(min)	Duration of an entry. ● For a local IP address, "--" is displayed. ● For a static entry, "static" is displayed. ● For a dynamic entry, the duration of the entry is displayed in minutes.
Hardware	Hardware address, that is, a 48-bit MAC address consisting of three parts separated by dots (.), with each part containing 16 bits. The address is expressed in hexadecimal notation.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.
Interface	Layer 3 interface corresponding to an ARP entry. Nothing is displayed if the IP address of a static ARP is not in any directly connected network segment of the device.
Origin	Source of a static ARP entry. ● **Configure** indicates that the entry is manually configured. ● **Authentication** indicates that the entry is generated via authentication.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.41 show arp oob

Function

Run the **show arp oob** command to display the ARP cache on a management interface.

Syntax

show arp oob [*ip-address* [*mask*] | *mac-address* | **complete | incomplete | static**]

Parameter Description

ip-address: IP address whose ARP entries need to be displayed.

mask: Subnet mask. After this parameter is specified, ARP entries within the IP subnet will be displayed.

mac-address: MAC address whose ARP entries need to be displayed.

static: Displays all static ARP entries.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache on the management interface.

```
Hostname> enable
Hostname# show arp oob
Total Numbers of Arp: 7
Protocol  Address         Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   0        0013.20a5.7a5f  arpa   mgmt 0
Internet  192.168.195.67   0        001a.a0b5.378d  arpa   mgmt 0
Internet  192.168.195.65   0        0018.8b7b.713e  arpa   mgmt 0
Internet  192.168.195.64   0        0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.63   0        001a.a0b5.3990  arpa   mgmt 0
Internet  192.168.195.62   0        001a.a0b5.0b25  arpa   mgmt 0
Internet  192.168.195.5    --       00d0.f822.33b1  arpa   mgmt 0
```

The following example displays the ARP entry of IP address 192.168.195.68 on the management interface.

```
Hostname> enable
Hostname# show arp oob 192.168.195.68
```

```
Protocol  Address         Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   1        0013.20a5.7a5f  arpa   mgmt 0
```

The following example displays ARP entries of IP subnet 92.168.195.0/24 on the management interface.

```
Hostname> enable
Hostname# show arp 192.168.195.0 255.255.255.0
Protocol  Address        Age(min)  Hardware       Type   Interface
Internet  192.168.195.64   0       0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.2    1       00d0.f8ff.f00e  arpa   mgmt 0
Internet  192.168.195.5    --      00d0.f822.33b1  arpa   mgmt 0
Internet  192.168.195.1    0       00d0.f8a6.5af7  arpa   mgmt 0
Internet  192.168.195.51   1       0018.8b82.8691  arpa   mgmt 0
```

The following example displays the ARP entry of MAC address 001a.a0b5.378d on the management interface.

```
Hostname> enable
Hostname# show arp 001a.a0b5.378d
Protocol  Address         Age(min)  Hardware       Type   Interface
Internet  192.168.195.67   4        001a.a0b5.378d  arpa   mgmt 0
```

Table 1-2 Output Fields of the show arp oob Command

Field	Description
Protocol	Protocol. **Internet** indicates the Internet protocol.
Address	IPv4 address.
Age(min)	Duration of an entry. ● For a local IP address, "--" is displayed. ● For a static entry, "static" is displayed. For a dynamic entry, the duration of the entry is displayed in minutes.
Hardware	Hardware address, that is, a 48-bit MAC address consisting of three parts separated by dots (.), with each part containing 16 bits. The address is expressed in hexadecimal notation.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.
Interface	Layer 3 interface corresponding to an ARP entry. Nothing is displayed if the IP address of a static ARP is not in any directly connected network segment of the device.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 show arp counter

Function

Run the **show arp counter** command to display the number of ARP entries in the ARP cache.

Syntax

show arp counter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the number of ARP entries in the ARP cache, including static ARP entries and dynamic ARP entries.

Examples

The following example displays the number of ARP entries in the ARP cache.

```
Hostname> enable
Hostname# show arp counter
ARP Limit:             75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1  incomplete: 0)
Total:                 1
```

Table 1-3 Output Fields of the show arp counter Command

Field	Description
ARP Limit	ARP capacity limit.
Count of static entries	Number of static entries.
Count of dynamic entries	Number of dynamic entries.
complete	Number of resolved ARP entries.
incomplete	Number of unresolved ARP entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 show arp detail

Function

Run the **show arp detail** command to display the details about the ARP cache.

Syntax

show arp detail [*interface-type interface-number* | **trusted** [*ip-address* [*mask*]] | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **complete** | **incomplete | static**] | **subvlan** { **min-max** *min-value max-value* | *subvlan-number* }]

Parameter Description

interface-type interface-number: *interface-type* indicates the interface type and *interface-number* indicates the interface number. After the parameter is specified, the ARP entries of a specified Layer 3 interface or Layer 2 interface are displayed.

vrf *vrf-name*: Displays ARP entries of a specified VRF instance.

trusted: Displays trusted ARP entries. Currently, only the global VRF instance supports trusted ARP entries.

ip-address: IP address whose ARP entries need to be displayed.

mask: Subnet mask. After this parameter is specified, ARP entries of a specified network segment will be displayed.

mac-address: MAC address whose ARP entries need to be displayed.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

static: Displays all static ARP entries.

subvlan: Displays ARP entries of a specified sub VLAN.

min-max: Displays the maximum and minimum values of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

min-value: Minimum value of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

max-value: Maximum value of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

subvlan-number: Sub VLAN ID. After this parameter is specified, ARP entries of a specified single sub VLAN will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the details about the ARP cache, including the type of ARP entries (dynamic, static, local, or trusted entries) and the Layer 2 ports.

Note

If the entered *min-value* is greater than *max-value*, no error is displayed, and ARP entries in the specified sub VLAN range are displayed.

Examples

The following example displays the details about the ARP cache.

```
Hostname> enable
Hostname# show arp detail
IP Address     MAC Address      Type      Age(min)   Interface  Port     SubVlan   Gid
20.1.1.2       0020.0101.0002   Static     --        Te2/5      --       --       0
20.1.1.1       00d0.f822.33bb   Local      --        Te2/5      --       --       0
1.1.1.2        00d0.1111.1112   Dynamic    1         Vl2        Te2/1    4        0
1.1.1.1        00d0.f822.33bb   Local      --        Vl2        --       --       0
```

Table 1-4 Output Fields of the show arp detail Command

Field	Description
IP Address	IP address corresponding to a hardware address.
MAC Address	Hardware address corresponding to the IP address.
Type	ARP entry types, including static, dynamic, trusted, and local.
Age	ARP aging time, in minutes.
Interface	Layer 3 interface associated with an IP address.
Port	Layer 2 port associated with an ARP entry.
SubVlan	Sub VLAN associated with an ARP entry.
Gid	IMLAG group ID.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show arp**

1.44 show arp packet statistics

Function

Run the **show arp packet statistics** command to display ARP packet statistics.

Syntax

show arp packet statistics [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface name. After this parameter is specified, the ARP packet statistics of a specified interface will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP packet statistics of all interfaces.

```
Hostname> enable
Hostname# show arp packet statistics
Interface            Received  Received Received  Sent     Sent
Name                Requests  Replies  Others    Requests  Replies
--------   ----  -------  ----  ---
GigabitEthernet 0/0    0        0       0        0        0
GigabitEthernet 0/1    143649    232     0        2        0
GigabitEthernet 0/2    0        0       0        0        0
GigabitEthernet 0/3    0        0       0        0        0
GigabitEthernet 0/4    0        0       0        0        0
GigabitEthernet 0/5    0        0       0        0        0
GigabitEthernet 0/6    0        0       0        0        0
Loopback 1           0        0       0        0        0
```

Table 1-5 Output Field of the show arp packet statistics Command

Field	Description
Interface Name	Interface name.
Received Requests	Number of received ARP requests.
Received Replies	Number of received ARP replies.

Field	Description
Received Others	Number of received other ARP packets.
Sent Requests	Number of sent ARP requests.
Sent Replies	Number of sent ARP replies.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show arp rate-statistic

Function

Run the **show arp rate-statistic** command to display the ARP packet rate statistics.

Syntax

show arp rate-statistic [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface ID. After this parameter is specified, the statistics on ARP packets of a specified interface will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display the ARP packet rate statistics (including received ARP requests, received ARP replies, received other ARP packets, sent ARP requests, and sent ARP replies).

Examples

The following example displays the ARP packet rate statistics of all interfaces.

```
Hostname> enable
Hostname(config)# show arp rate-statistic
Interface Sampling Received    Received    Received    Sent        Sent
Name      time     Requests(pps) Replies(pps) Others(pps) Requests(pps) Replies(pps)
```

```
--------     ----     ----     ----     ----     ---
TenGigabitEthernet 0/15    1    0     0         0        1      0
Mgmt 0                   1    7     0         0        0      0
```

The following example displays the ARP packet rate statistics of SVI 1.

```
Hostname> enable
Hostname(config)# show arp rate-statistic interface vlan 1
Interface Sampling Received    Received    Received    Sent         Sent
Name      time    Requests(pps) Replies(pps) Others(pps) Requests(pps) Replies(pps)
--------      ----     ----     ----     ----     ----     ---
VLAN 1     1         0              0           0            0            0
```

Table 1-6 Output Field of the show arp rate-statistic Command

Field	Description
Interface Name	Interface name.
Sampling time	Sampling time.
Received Requests(pps)	Rate of received ARP requests.
Received Replies(pps)	Rate of received ARP replies.
Received Others(pps)	Rate of received other ARP packets.
Sent Requests(pps)	Rate of sent ARP requests.
Sent Replies(pps)	Rate of sent ARP replies.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Related Commands

N/A

1.46 show arp timeout

Function

Run the **show arp timeout** command to display the aging time of dynamic ARP entries.

Syntax

show arp timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the aging time of dynamic ARP entries.

```
Hostname> enable
Hostname# show arp timeout
Interface            arp timeout(sec)
--------  ------
VLAN 1               3600
```

Table 1-7 Output Fields of the show arp timeout Command

Field	Description
Interface	Interface name.
arp timeout(sec)	Aging time of ARP entries, in seconds.

Notifications

N/A

Platform Description

N/A

Related Commands

- **arp timeout**

1.47 show arp flapping record

Function

Run the **show arp flapping record** command to display ARP flapping records.

Syntax

show arp flapping record [*ipv4-address*]

Parameter Description

***ipv4-address*: ARP records of the specified IPv4 address. Command Modes**

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

ARP flapping occurs when a device learns an entry with the same IP address twice but the MAC addresses are different.

Examples

The following example displays ARP flapping records.

```
Hostname> enable
Hostname# show arp flapping record
Hostname> enable
Hostname# show arp flapping record
Arp flapping recorded:
  Arp flapping record max count: 10240
  Arp flapping record current count: 2
  Arp flapping record history count: 2
  Move-Time                ip-address        Original-Mac        Move-Mac
Port             Vid
  1970/01/02 02:54:20        192.168.193.52    300d.9e15.bda1      00d0.f822.358b
--               0
  1970/01/02 03:39:20        192.168.193.59    300d.9e15.bda1      00d0.f822.33f8
--               0
Total flapping record: 2
```

Table 1-8 Output Field of the show arp flapping record Command

Field	Description
Arp flapping recorded	ARP flapping records.
Arp flapping record max count	Maximum count of ARP flapping records.
Arp flapping record history count	Historical count of ARP flapping records.
Move-Time	Flapping occurrence time.

Field	Description
Ip-address	ARP IP address where flapping occurs.
Original-Mac	ARP MAC address before flapping.
Move-Mac	ARP MAC address after flapping.
Port	ARP outbound interface where flapping occurs.
Vid	ARP VLAN ID where flapping occurs.
Total flapping record	Total number of ARP flapping records.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 show ip arp

Function

Run the **show ip arp** command to display the ARP cache.

Syntax

show ip arp [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Displays the ARP entries of a specified VRF instance.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache.

```
Hostname> enable
Hostname# show ip arp
```

```
Protocol Address      Age(min)Hardware       Type
Interface
Internet 192.168.7.233  23   0007.e9d9.0488  ARPA GigabitEthernet 0/0
Internet 192.168.7.112  10   0050.eb08.6617  ARPA GigabitEthernet 0/0
Internet 192.168.7.79   12   00d0.f808.3d5c  ARPA GigabitEthernet 0/0
Internet 192.168.7.1    50   00d0.f84e.1c7f  ARPA GigabitEthernet 0/0
Internet 192.168.7.215  36   00d0.f80d.1090  ARPA GigabitEthernet 0/0
Internet 192.168.7.127  0    0060.97bd.ebee  ARPA GigabitEthernet 0/0
Internet 192.168.7.195  57   0060.97bd.ef2d  ARPA GigabitEthernet 0/0
Internet 192.168.7.183  --   00d0.f8fb.108b  ARPA GigabitEthernet 0/0
```

The following example displays the ARP entries of a VRF instance named vpnv4.

```
Hostname> enable
Hostname# show ip arp vrf vpnv4
Protocol  Address         Age(min)  Hardware       Type   Interface
Internet  11.1.1.1        0         78e3.b5b6.f4dc  arpa   GigabitEthernet 0/0
Internet  11.1.1.2        --        1111.2222.1111  arpa   GigabitEthernet 0/0
Total number of ARP entries: 2
```

Table 1-9 Output Fields of the show ip arp Command

Field	Description
Protocol	Network address protocol. This field is always **Internet**.
Address	IP address corresponding to a hardware address.
Age(min)	Aging time of ARP cache records, in minutes. For local or static entries, this field is filled with a hyphen (-).
Hardware	Hardware address corresponding to the IP address.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.
Interface	Interface associated with an IP address.
Total number of ARP entries	Total number of ARP entries.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show arp**

1.49 show arp anti-attack statistics

Function

Run the **show arp anti-attack statistics** command to display the statistics on illegal ARP packets.

Syntax

show arp anti-attack statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the statistics on illegal ARP packets.

```
Hostname> enable
Hostname# show arp anti-attack statistics
Number of ARP packet(s) dropped by strict learning:       55
Number of ARP packet(s) dropped by sender-mac checking:    5
Number of ARP packet(s) dropped by target-mac checking:    66
Number of ARP packet(s) dropped by gratuitous checking:    101
Number of ARP packet(s) dropped by acl checking:          7
Number of ARP packet(s) dropped by hardware-type checking:  2
Number of ARP packet(s) dropped by hardware-size checking:  9
Number of ARP packet(s) dropped by protocol-type checking:  78
Number of ARP packet(s) dropped by protocol-size checking:  11
Number of ARP packet(s) dropped by opcode checking:       35
Number of ARP packet(s) dropped by ip checking:           0
```

Table 1-10 Output Field of the show arp anti-attack statistics Command

Field	Description
Number of ARP packet(s) dropped by strict learning	Number of illegal ARP packets that are dropped due to strict learning.
Number of ARP packet(s) dropped by sender-mac checking	Number of illegal ARP packets that are dropped due to source MAC address check carried by the sender.
Age (Number of ARP packet(s) dropped by target-mac checking)	Number of illegal ARP packets that are dropped due to destination MAC address check.

Field	Description
Number of ARP packet(s) dropped by gratuitous checking	Number of illegal ARP packets that are dropped due to gratuitous ARP check.
Number of ARP packet(s) dropped by acl checking	Number of illegal ARP packets that are dropped due to ACL check.
Number of ARP packet(s) dropped by hardware-type checking	Number of illegal ARP packets that are dropped due to hardware type check.
Number of ARP packet(s) dropped by hardware-size checking	Number of illegal ARP packets that are dropped due to hardware size check.
Number of ARP packet(s) dropped by protocol-type checking	Number of illegal ARP packets that are dropped due to protocol type check.
Number of ARP packet(s) dropped by protocol-size checking	Number of illegal ARP packets that are dropped due to protocol size check.
Number of ARP packet(s) dropped by opcode checking	Number of illegal ARP packets that are dropped due to operation code check.
Number of ARP packet(s) dropped by ip checking	Number of illegal ARP packets that are dropped due to IP address check.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

-

1 IPv4 Basics Commands

Command	Function
gateway	Configure the default gateway for a management interface.
ip address	Configure an IP address for an interface.
ip address mix	Configure an IP address combination.
ip address negotiate	Configure an interface to obtain the IP address through the Point to Point Protocol (PPP) negotiation.
ip broadcast-address	Configure a broadcast address for an interface.
ip icmp error-interval	Configure the transmission rate of Internet Control Message Protocol (ICMP) error packets.
ip icmp timestamp	Configure the timestamp query function.
ip directed-broadcast	Enable the translation of the IP directed broadcast mode to the physical broadcast mode.
ip mask-reply	Enable the function of sending ICMP mask reply messages.
ip mtu	Configure the maximum transmission unit (MTU) for an IP packet.
ip redirects	Enable the function of sending ICMP redirection messages.
ip redirect-drop	Enable the routed port protection function.
ip source-route	Enable the function of processing IP source routing information.
ip ttl	Configure a time to live (TTL) value for unicast packets sent by the device.
ip ttl-expires enable	Enable the device to send a TTL timeout message.
ip unnumbered	Enable an unnumbered interface to borrow an IP address.
ip unreachables	Enable the function of sending ICMP destination unreachable messages.

show ip interface	Display the IP status of an interface.
show ip packet queue	Display statistics on sent and received IP packets in the protocol stack.
show ip packet statistics	Display the statistics on IP packets.
show ip raw-socket	Display all the IPv4 raw sockets.
show ip sockets	Display all IPv4 sockets.
show ip udp	Display all IPv4 UDP sockets.
show ip udp statistics	Display the number of IPv4 UDP sockets.

1.1 gateway

Function

Run the **gateway** command to configure the default gateway for a management interface.

Run the **no** form of this command to remove this configuration.

No default gateway is configured for a management interface by default.

Syntax

gateway *ip-address*

no gateway

Parameter Description

ip-address: Default gateway of a management interface for Internet Protocol version 4 (IPv4) communication.

Command Modes

MGMT interface mode

Default Level

2

Usage Guidelines

The type of a management interface is MGMT and the interface number is fixed to 0.

Examples

The following example sets the default gateway of a MGMT interface to 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-Mgmt 0)# gateway 1.1.1.1
```

Notifications

When the configured IP address is illegal, the following notification will be displayed:

```
% 0.0.0.0 is not a valid host address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.2 ip address

Function

Run the **ip address** command to configure an IP address for an interface.

Run the **no** form of this command to remove this configuration.

No IP address is configured for an interface by default.

Syntax

ip address *ip-address mask* [**secondary**]

no ip address [*ip-address mask* [**secondary**]

Parameter Description

ip-address: IP address consisting of 32 bits, with 8 bits for each group. The IP address is expressed in dotted decimal notation.

mask: Network mask consisting of 32 bits. Value **1** indicates the mask bit and **0** indicates the host bit. Every 8 bits form one group. The network mask is expressed in dotted decimal notation.

secondary: Configures an IP address as a secondary IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

A device can receive and send IP packets only after the device is configured with an IP address.

A network mask is also a 32-bit value and identifies the bits occupied by the network part of an IP address. In a network mask, the bits whose values are ones are for the network part, and the bits whose values are zeros are for host addresses. For example, for class A networks, the network mask is 255.0.0.0. Subnetting allows you to divide a network into several subnets. You can use some bits of the host address as the network ID to decrease the host capacity and increase the number of networks. In this case, network masks are called subnet masks.

The device supports multiple IP addresses on one interface, of which one is the primary IP address and the others are secondary IP addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, when the number of hosts exceeds 254 in a local area network (LAN), one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on Layer 2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, in consideration that one subnet cannot

be configured on two or more interfaces of a device, you can connect the isolated subnets by creating a subnet on the isolated network and configuring a secondary address.

Examples

The following example sets the primary IP address to 10.10.10.1, subnet mask to 255.255.255.0, and default gateway to 10.10.10.254, for port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0 gateway
10.10.10.254
```

Notifications

Do not set the mask to all ones or zeros (32-bit mask is supported for loopback interfaces). Otherwise, the following notification will be displayed:

```
Invalid IP mask.
```

Do not configure a secondary IP address if a primary IP address is not configured. Otherwise, the following notification will be displayed:

```
Cannot add IP address.
```

Common Errors

- A secondary IP address is configured when no primary IP address is configured.
- Network segments of different IP addresses overlap on the same interface.

Platform Description

N/A

Related Commands

- **show ip interface**
- **gateway**
- **ip default-gateway** (IP routing/static routing)

1.3 ip address mix

Function

Run the **ip address mix** command to configure an IP address combination.

Run the **no** form of this command to remove this configuration.

No IP address combination is configured for an interface by default.

Syntax

ip address mix { **dhcp** | *ip-address network-mask* }

no ip address mix { **dhcp** | *ip-address network-mask* }

Parameter Description

dhcp: Obtains a dynamic IP address through the Dynamic Host Configuration Protocol (DHCP).

ip-address: IP address consisting of 32 bits, with 8 bits for each group. The IP address is expressed in dotted decimal notation.

network-mask: Network mask, consisting of 32 bits, with 8 bits for each group. Value **1** indicates the mask bit and **0** indicates the host bit. The network mask is expressed in dotted decimal notation.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The IP address combination configuration command can be configured only on switch virtual interfaces (SVIs) and MGMT interfaces.

The IP address combination configuration command, static IP configuration command, and dynamic IP configuration command are mutually exclusive. However, the IP address combination configuration command can be used to configure both static IP addresses and DHCP to obtain dynamic IP addresses.

- When the IP address combination configuration command is used to configure a static IP address, if an IP address in the same network segment is already configured, the configuration fails.
- When the IP address combination configuration command is used to configure both a static IP address and a dynamic IP address, if the dynamic IP address obtained through DHCP does not conflict with the network segment of the static IP address, the dynamic IP address is the primary IP address and the static IP address is a secondary IP address. If the dynamic IP address obtained through DHCP conflicts with the network segment of the static IP address, an IP address will be obtained again, during which the static IP address is a primary IP address.

Examples

The following example sets the IP address combination to 192.168.23.110/24 and DHCP on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip address mix dhcp
Hostname(config-if-VLAN 1)# ip address mix 192.168.23.110 255.255.255.0
```

Notifications

N/A

Common Errors

- The IP address combination configuration command is configured after the static or dynamic IP command is configured.
- This command is used on non-SVI interfaces and non-MGMT interfaces.

Platform Description

N/A

Related Commands

- **show ip interface**

1.4 ip address negotiate

Function

Run the **ip address negotiate** command to configure an interface to obtain the IP address through the Point to Point Protocol (PPP) negotiation.

Run the **no** form of this command to remove this configuration.

No interface is configured to obtain an IP address through the PPP negotiation by default.

Syntax

ip address negotiate

no ip address negotiate

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When **ip address negotiate** is configured on an interface, **peer default ip address** needs to be configured on the peer.

Examples

The following example configures the interface Dialer 1 to obtain an IP address through the PPP negotiation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface dialer 1
Hostname(config-if-dialer 1)# ip address negotiate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **encapsulation ppp** (interfaces/Ethernet interfaces)

1.5 ip broadcast-address

Function

Run the **ip broadcast-address** command to configure a broadcast address for an interface.

Run the **no** form of this command to remove this configuration.

The default IP broadcast address is 255.255.255.255.

Syntax

ip broadcast-address *ip-address*

no ip broadcast-address

Parameter Description

ip-address: Broadcast address of an IP network.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Generally, the destination address of IP broadcast packets is all ones, which is expressed as 255.255.255.255. Users can define other IP addresses as broadcast addresses to receive the broadcast packets with the address 255.255.255.255 and user-defined broadcast packets.

Examples

The following example sets the broadcast address of port GigabitEthernet 0/1 to 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip broadcast-address 1.1.1.1
```

Notifications

Do not configure a broadcast address if no primary IP address is configured for an interface. Otherwise, the following notification will be displayed:

```
Cannot set broadcast address. No primary address exist.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip address**

1.6 ip icmp error-interval

Function

Run the **ip icmp error-interval** command to configure the transmission rate of Internet Control Message Protocol (ICMP) error packets.

Run the **no** form of this command to restore the default configuration.

Ten ICMP error packets are transmitted within 100 ms by default.

Syntax

ip icmp error-interval [**df**] *interval* [*bucket-size*]

no ip icmp error-interval [**df**] *interval* [*bucket-size*]

Parameter Description

df: Configures the transmission rate of ICMP destination unreachable packets triggered by the don't fragment (DF) bit in the IP header.

interval: Refresh cycle of a token bucket, in ms. The value range is from 0 to 2147483647, and the default value is **100**. When the value is **0**, the transmission rate of ICMP error packets is not limited.

bucket-size: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is **10**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This function limits the transmission rate of ICMP error packets by using the token bucket algorithm to prevent denial of service (DoS) attacks.

If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable message to the source host. This ICMP error packet is used to discover the path MTU. If there are too many other ICMP error packets, the ICMP destination unreachable packet may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively.

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the transmission rate is set to 1 packet per 5 milliseconds, two ICMP errors are actually sent per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the transmission rate is set to 3 packets per 15 milliseconds, two ICMP errors are actually sent per 10 milliseconds.

Examples

The following example sets the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header to 100 packets per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip icmp error-interval DF 1000 100
```

The following example sets the transmission rate of other ICMP error packets to 10 packets per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip icmp error-interval 1000 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip icmp timestamp**

1.7 ip icmp timestamp

Function

Run the **ip icmp timestamp** command to configure the timestamp query function.

Run the **no** form of this command to remove this configuration.

The timestamp query function is enabled by default.

Syntax

ip icmp timestamp

no ip icmp timestamp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

RFC792 requires the system to return its current time after receiving an ICMP timestamp query.

To prevent attackers from obtaining the system time through this protocol and attacking some time-based protocols, you can disable the timestamp query function. Then the device directly discards received ICMP timestamp query requests.

Examples

The following example disables the timestamp query function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip icmp timestamp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip packet queue**
- **show ip packet statistics**

1.8 ip directed-broadcast

Function

Run the **ip directed-broadcast** command to enable the translation of the IP directed broadcast mode to the physical broadcast mode.

Run the **no** form of this command to disable this feature.

The function of translating the IP directed broadcast mode into the physical broadcast mode is disabled by default.

Syntax

ip directed-broadcast [*acl-number*]

no ip directed-broadcast

Parameter Description

acl-number: No. of an access control list (ACL). The value range is from 1 to 199 and 1300 to 2699. After an ACL is defined, conversion is performed only for directed broadcast packets that match the ACL. No ACL is defined by default and translation is performed for all broadcast packets in subnets.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

IP directed broadcast packets refer to the IP packets destined for a broadcast address in an IP subnet. However, the node that generates the packets is not a member of the destination subnet.

After receiving IP directed broadcast packets, the devices not directly connected to the destination subnet forward the broadcast packets in the same way as that for unicast packets. After directed broadcast packets reach the device directly connected to the destination subnet, the device translates the directed broadcast mode into limited broadcast mode (with a destination IP address being 255.255.255.255) and broadcasts the packets to all hosts on the destination subnet at the link layer.

After the function of translating the directed broadcast mode into the physical broadcast mode is enabled on a specified interface, the interface can forward the directed broadcast packets from the directly connected network. This command affects only the final transmission of directed broadcast packets within destination subnet and will not affect the forwarding of other directed broadcast packets.

On an interface, you can also define an ACL to forward desired directed broadcast packets. After an ACL is defined, only data packets that match the ACL are subject to the translation from the directed broadcast mode to physical broadcast mode.

If the **no ip directed-broadcast** command is run on an interface, the device will discard directed broadcast packets received from the directly connected network.

Examples

The following example enables the translation from directed broadcast mode to physical broadcast mode on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip broadcast-address

1.9 ip mask-reply

Function

Run the **ip mask-reply** command to enable the function of sending ICMP mask reply messages.

Run the **no** form of this command to disable this feature.

The function of sending ICMP mask reply messages is enabled by default.

Syntax

ip mask-reply

no ip mask-reply

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When a network device sends an ICMP mask request message to obtain the mask of a subnet, the network device that receives the ICMP mask request message returns a mask reply message.

Examples

The following example enables the function of sending ICMP mask reply messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip mask-reply
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ip interface

- **show ip packet queue**
- **show ip packet statistics**

1.10 ip mtu

Function

Run the **ip mtu** command to configure the maximum transmission unit (MTU) for an IP packet.

Run the **no** form of this command to restore the default configuration.

The default MTU of an IP packet is 1500 bytes.

Syntax

ip mtu *mtu*

no ip mtu

Parameter Description

mtu: MTU of an IP packet, in bytes. The value range is from 68 to 1500.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If the size of an IP packet exceeds the IP MTU value, the packet will be fragmented. For all devices on the same physical network segment, the IP MTU configured for the interconnected interfaces must be the same.

If the MTU value of an interface is set by running the **mtu** command, the IP MTU value will be automatically kept the same as that of interfaces. However, if the IP MTU value is adjusted, the MTU value of interfaces will not change accordingly.

Examples

The following example sets the IP MTU of port GigabitEthernet 0/1 to 512 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip mtu 512
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **mtu** (interfaces/Ethernet interfaces)

1.11 ip redirects

Function

Run the **ip redirects** command to enable the function of sending ICMP redirection messages.

Run the **no** form of this command to disable this feature.

The function of sending ICMP redirection messages is enabled by default.

Syntax

ip redirects

no ip redirects

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When a route is less than optimal, a device may send packets through an interface that receives the packets. If the function of sending ICMP redirection messages is enabled, when the device sends the packets from the interface that receives the packets, the device sends an ICMP redirection message to the source to inform that the gateway reachable to the destination address is another device on the same subnet. In this way, the source sends subsequent packets along the optimal path.

Examples

The following example disables the function of sending ICMP redirection messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip redirects
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.12 ip redirect-drop

Function

Run the **ip redirect-drop** command to enable the routed port protection function.

Run the **no** command to disable this feature.

The routed port protection function is disabled by default.

Syntax

ip redirect-drop

no ip redirect-drop

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The routed port protection function is enabled on an interface to prevent packets from being transmitted through the same interface that receives the packets.

Examples

The following example enables the routed port protection function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip redirect-drop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.13 ip source-route

Function

Run the **ip source-route** command to enable the function of processing IP source routing information.

Run the **no** form of this command to disable this feature.

The function of processing IP source routing information is enabled by default.

Syntax

ip source-route

no ip source-route

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When a device receives an IP packet, it checks the options such as the strict source route, loose source route, and record route in the IP packet header. These options are detailed in RFC 791. If the device detects that the packet enables one option, it performs an action accordingly; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the source route option is enabled, you can test the throughput of a specific network or help the packet bypass the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

Examples

The following example disables the function of processing IP source routing information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip source-route
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.14 ip ttl

Function

Run the **ip ttl** command to configure a time to live (TTL) value for unicast packets sent by the device.

Run the **no** form of this command to remove this configuration.

The default TTL value of the unicast packets sent by the device is 64.

Syntax

ip ttl *ttl*

no ip ttl

Parameter Description

ttl: TTL value of the unicast packets sent by the device. The value range is from 1 to 255.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When an IP packet is transmitted from the source address to the destination address through routers, if a TTL value is set, the TTL value decreases by 1 each time the IP packet passes through a router. When the TTL value drops to zero, the router discards the packet. TTL prevents infinite transmission of useless packets and waste of bandwidth.

Examples

The following example sets the TTL of unicast packets sent by the device to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ttl 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.15 ip ttl-expires enable

Function

Run the **ip ttl-expires enable** command to enable the device to send a TTL timeout message.

Run the **no** form of this command to disable this feature.

The function of sending TTL timeout messages is enabled by default.

Syntax

ip ttl-expires enable

no ip ttl-expires enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When forwarding an IP packet whose TTL expires, a device responds to the source end with a TTL timeout error message.

To prevent attacks from other devices after the device is located through traceroute, you can disable the function of sending TTL timeout error messages on the device. When this function is disabled, the device will no longer make a response when receiving a TTL timeout message.

Examples

The following example disables the function of sending TTL timeout messages on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip ttl-expires enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.16 ip unnumbered

Function

Run the **ip unnumbered** command to enable an unnumbered interface to borrow an IP address.

Run the **no** form of this command to remove this configuration.

No unnumbered interface is configured to borrow an IP address by default.

Syntax

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

An unnumbered interface is an interface that is enabled with the IP protocol but has no IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address for communication. For an IP packet generated by an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface based on the associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations:

- An Ethernet interface cannot be configured as an unnumbered interface.
- When the Serial Line Internet Protocol (SLIP), High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), or frame relay is configured on a serial interface, the serial interface can be configured as an unnumbered interface. When frame relay is configured, only a point-to-point subinterface can be configured as an unnumbered interface. An X.25 interface cannot be configured as an unnumbered interface.

- The ping tool cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface has no IP address.
- You can monitor the status of an unnumbered interface remotely through the Simple Network Management Protocol (SNMP).
- Network startup cannot be carried out through an unnumbered interface.

Examples

The following example configures the unnumbered interface Virtual-ppp 1 to associate with the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)# ip unnumbered gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.17 ip unreachables

Function

Run the **ip unreachables** command to enable the function of sending ICMP destination unreachable messages.

Run the **no** form of this command to disable this feature.

The function of sending ICMP destination unreachable messages is enabled by default.

Syntax

ip unreachables

no ip unreachables

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If a device receives a unicast packet destined for itself and finds that it cannot process the upper layer protocol of the packet, the device returns an ICMP protocol unreachable message to the data source.

If the device does not know a route to forward packets, it also returns an ICMP host unreachable message to the data source.

This command affects all ICMP destination unreachable messages.

Examples

The following example disables the function of sending ICMP destination unreachable messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip unreachables
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.18 show ip interface

Function

Run the **show ip interface** command to display the IP status of an interface.

Syntax

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

interface-type interface-number: Interface type and interface number.

brief: Displays the basic IP configurations of an L3 interface, including primary/secondary IP addresses and interface status.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

If an interface can receive and transmit a data packet, the interface is available, and the device software will create a direct route in the routing table. If the interface becomes unavailable, the software will delete the direct route from the routing table.

If an interface is available, the status of the line protocol will be displayed as "up". If only a physical line is available, the status of the interface will be displayed as "up".

The displayed result may be different depending on the interface type because some options are specific to certain interfaces.

Examples

The following example displays the IP status of all interfaces.

```
Hostname> enable
Hostname# show ip interface brief
Interface          IP-Address(Pri)  IP-Address(Sec) Status Protocol
GigabitEthernet 0/10  2.2.2.2/24     3.3.3.3/24    down   down
GigabitEthernet 0/11  no address     no address    down   down
VLAN 1                1.1.1.1/24     no address    down   down
```

Table 1-1 Output Fields of the show ip interface brief Command

Field	Description
Interface	Interface name.
IP-Address(Pri)	Primary IP address and mask of an interface.
IP-Address(Sec)	Secondary IP address and mask of an interface.
Status	Link status of an interface. ● **Up**: Indicates that an interface is up. ● **Down**: Indicates that an interface is down. **administratively down**: A user runs the **shutdown** command to forcibly shut down an interface.
Protocol	IPv4 protocol status of an interface.

The following example displays the IP status of interface VLAN 1.

```
Hostname> enable
Hostname# show ip interface vlan 1
VLAN 1
```

```
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  Proxy ARP is: OFF
ARP packet input number:          0
    Request packet:               0
    Reply packet:                 0
    Unknown packet:               0
TTL invalid packet number:          0
ICMP packet input number:          0
    Echo request:                 0
    Echo reply:                   0
    Unreachable:                  0
    Source quench:                0
    Routing redirect:                0
```

Table 1-2 Output Fields of the show ip interface Command

Field	Description
IP interface state is	Status of a network interface. ● **Down**: Indicates that an interface is unavailable, with the hardware status or line protocol status being down. **Up**: Indicates that an interface is available, with both the hardware status and line protocol status being up.
IP interface type is	Interface type, such as broadcast and point-to-point.
IP interface MTU is	MTU value set for an interface.
IP address is	IP address and mask of an interface.
IP address negotiate is	Whether the IP address of an interface is obtained by negotiation.
Forward direct-broadcast is	Whether an interface forwards directed broadcast packets.
ICMP mask reply is	Whether an interface sends an ICMP mask reply packet.
Send ICMP redirect is	Whether an interface sends an ICMP redirection packet.
Send ICMP unreachable is	Whether an interface sends an ICMP unreachable packet.

Field	Description
Proxy ARP is	Whether proxy ARP is enabled.
ARP packet input number	Total number of ARP packets received on an interface, including: ● **Request packet**: Indicates ARP request packets. ● **Reply packet**: Indicates ARP reply packets. ● **Unknown packet**: Indicates unknown packets.
TTL invalid packet number	Number of invalid TTL packets received on an interface.
ICMP packet input number	Total number of ICMP packets received on an interface, including: ● **Echo request**: Indicates echo request packets. ● **Echo reply**: Indicates echo reply packets. ● **Unreachable**: Indicates unreachable packets. ● **Source quench**: Indicates source quench packets. ● **Routing redirect**: Indicates routing redirection packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show ip packet queue

Function

Run the **show ip packet queue** command to display statistics on sent and received IP packets in the protocol stack.

Syntax

show ip packet queue

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display statistics on sent and received IP packets in the protocol stack.

Examples

The following example displays the statistics on sent and received IP packets in the protocol stack.

```
Hostname> enable
Hostname# show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
Failed to alloc efbuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Get vrf fails: 0
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
```

Table 1-3 Output Fields of the show ip packet queue Command

Field	Description
IP packet receive queue	IP packet receiving queue in the protocol stack.
Discards	Packets that are dropped during receiving.
Failed to alloc skb	Number of packets dropped due to the receiving thread allocation failure.
Receive queue overflow	Number of packets that are dropped due to queue overflow.
Unknow protocol drops	Number of packets that are dropped because there is no corresponding protocol available for receiving.
ICMP rcv drops: x. for skb check fail.	The number of packets with ICMP checksum error is x.

Field	Description
ICMP rcv drops: x. for skb is broadcast.	The number of broadcast packets dropped by ICMP is x.
Sent packets	Statistics on sent IP packets.
Success	Number of packets successfully sent by the upper layer.
It records x us as max time in ICMP reply process.	The maximum time in the ICMP reply process is x μs.
Failed to alloc efbuf	Failure count of conversion from the socket buffer into expedited forwarding buffer.
Dropped by EFMP	Statistics on transmission failures.
NoRoutes	Number of packets dropped due to a lack of routes.
Get vrf fails	Count of the failures of getting the VRF instance bound to an interface.
Cannot assigned address drops	Number of packets dropped due to address allocation failures.
Failed to encapsulate ethernet head	Number of packets that fail in the Layer 2 header encapsulation.
ICMP error queue	Receiving queue of ICMP error packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ip packet statistics

Function

Run the **show ip packet statistics** command to display the statistics on IP packets.

Syntax

show ip packet statistics [**total** | *interface-type interface-number*]

Parameter Description

total: Displays the sum of statistic values of all interfaces.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the statistics of IP packets of all interfaces.

Examples

The following example displays the statistics of IP packets of all interfaces.

```
Hostname> enable
Hostname# show ip packet statistics
Total
  Received 113962 packets, 11948991 bytes
    Unicast:90962,Multicast:5232,Broadcast:17768
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 34917 packets, 1863146 bytes
    Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
  Received 6715 packets, 416587 bytes
    Unicast:2482,Multicast:4233,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 6720 packets, 417096 bytes
    Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
Tunnel 1
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
```

```
    Others:0
  Sent 21584 packets, 1122848 bytes
Unicast:21584,Multicast:0,Broadcast:0
```

Table 1-4 Output Fields of the show ip packet statistics Command

Field	Description
Total	Sum of the statistic values of all interfaces.
GigabitEthernet 0/1	Statistics of a specific interface.
Received x packets, y bytes	x packets are received, with y bytes in total.
Sent x packets, y bytes	x packets are sent, with y bytes in total.
Unicast	Number of unicast packets.
Multicast	Number of multicast packets.
Broadcast	Number of broadcast packets.
Discards	Number of dropped packets.
HdrErrors	Number of error packets.
BadChecksum	Number of packets with checksum error.
TTLExceeded	Number of packets with the size exceeding the TTL value.
Others	Others
NoRoutes	Number of packets without routing.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show ip raw-socket

Function

Run the **show ip raw-socket** command to display all the IPv4 raw sockets.

Syntax

show ip raw-socket [*protocol-number*]

Parameter Description

protocol-number: Protocol number.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 raw sockets, including the protocol number and process name.

Examples

The following example displays all IPv4 raw sockets.

```
Hostname> enable
Hostname# show ip raw-socket
Number Protocol Process name
1      ICMP     dhcp.elf
2      ICMP     vrrp.elf
3      IGMP     igmp.elf
4      VRRP     vrrp.elf
Total: 4
```

Table 1-5 Output Fields of the show ip raw-socket Command

Field	Description
Number	No.
Protocol	Protocol number.
Process name	Process name.
Total	Total number.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show ip sockets

Function

Run the **show ip sockets** command to display all IPv4 sockets.

Syntax

show ip sockets

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 sockets and thus obtain the User Datagram Protocol (UDP) port and Transmission Control Protocol (TCP) port that provide services for external devices.

Examples

The following example displays all IPv4 sockets.

```
Hostname> enable
Hostname# show ip sockets
Number Process name    Type    Protocol LocalIP:Port ForeignIP:Port     State
1     dhcp.elf        RAW     ICMP    0.0.0.0:1    0.0.0.0:0             *
2     vrrp.elf        RAW     ICMP    0.0.0.0:1    0.0.0.0:0             *
3     igmp.elf        RAW     IGMP    0.0.0.0:2    0.0.0.0:0             *
4     vrrp.elf        RAW     VRRP    0.0.0.0:112   0.0.0.0:0             *
5     dhcpc.elf       DGRAM   UDP     0.0.0.0:68    0.0.0.0:0             *
6     rg-snmpd        DGRAM   UDP     0.0.0.0:161   0.0.0.0:0             *
7     wbav2          DGRAM   UDP     0.0.0.0:2000  0.0.0.0:0             *
8     vrrp_plus.elf   DGRAM   UDP     0.0.0.0:3333  0.0.0.0:0              *
9    rds_other_th    DGRAM   UDP     0.0.0.0:3799  0.0.0.0:0             *
10    rg-snmpd        DGRAM   UDP     0.0.0.0:14800 0.0.0.0:0              *
11    rg-sshd         STREAM  TCP     0.0.0.0:22    0.0.0.0:0             LISTEN
12    rg-telnetd      STREAM  TCP     0.0.0.0:23    0.0.0.0:0             LISTEN
13    wbard          STREAM  TCP     0.0.0.0:4389  0.0.0.0:0             LISTEN
14    wbard          STREAM  TCP     0.0.0.0:7165  0.0.0.0:0             LISTEN
Total: 14
```

Table 1-6 Output Fields of the show ip sockets Command

Field	Description
Number	No.

Field	Description
Process name	Process name.
Type	Socket type. ● **RAW** indicates a raw socket. ● **DGRAM** indicates the packet type. ● **STREAM** indicates the stream type.
Protocol	Protocol number.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	IP address and port of the peer.
State	Status (only for TCP sockets).
Total	Total number of sockets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 show ip udp

Function

Run the **show ip udp** command to display all IPv4 UDP sockets.

Syntax

show ip udp [**local-port** *port-number* | **peer-port** *port-number*]

Parameter Description

local-port *port-number*: Specifies a local port number.

peer-port *port-number*: Specifies a peer port number.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 UDP sockets. You can know the UDP port that provides services for external devices.

Examples

The following example displays all IPv4 UDP sockets.

```
Hostname> enable
Hostname# show ip udp
Number Local Address        Peer Address         Process name
1      0.0.0.0:68           0.0.0.0:0            dhcpc.elf
2      0.0.0.0:161          0.0.0.0:0            snmp_mib_cmd_pr
3      0.0.0.0:3784         0.0.0.0:0            bfd.elf
4      0.0.0.0:3785         0.0.0.0:0            bfd.elf
5      0.0.0.0:7784         0.0.0.0:0            bfd.elf
6      0.0.0.0:42011        0.0.0.0:0            snmpd
```

Table 1-7 Output Fields of the show ip udp Command

Field	Description
Number	No.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.24 show ip udp statistics

Function

Run the **show ip udp statistics** command to display the number of IPv4 UDP sockets.

Syntax

show ip udp statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the number of IPv4 UDP sockets.

```
Hostname> enable
Hostname# show ip udp statistics
Number of IPv4 UDP sockets is 4.
```

Table 1-8 Output Fields of the show ip udp Command

Field	Description
Number of IPv4 UDP sockets is x	Total number of IPv4 UDP sockets is x.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 DHCP Commands

Command	Function
address range	Configure the network segment of a class.
address-manage	Enter the AM rule configuration mode.
bootfile	Configure the boot image file name that a DHCP server assigns to a DHCP client.
class	Configure the class associated with a DHCP address pool.
clear match ip	Clear the matching rules in AM rules.
clear ip dhcp binding	Clear the DHCP IP address binding table.
clear ip dhcp conflict	Clear DHCP address conflict records.
clear ip dhcp history	Clear historical DHCP address records.
clear ip dhcp server detect	Clear rogue DHCP server detection records.
clear ip dhcp server rate	Clear statistics about the processing rate of DHCP server packets on related modules.
clear ip dhcp server statistics	Clear statistics of a DHCP server.
clear ip dhcp relay statistics	Clear statistics of a DHCP relay agent.
client-identifier	Configure a unique DHCP client ID.
client-name	Configure a DHCP client name.
default-router	Configure the default gateway that a DHCP server assigns to a DHCP client.
dns-server	Configure the Domain Name System (DNS) server that a DHCP server assigns to a DHCP client.
domain-name	Configure the domain name that a DHCP server assigns to a DHCP client.
force-no-router	Forcibly disable gateway assignment to a DHCP client.
hardware-address	Configure a hardware address for a DHCP client.
host	Configure the IP address and network mask of a DHCP client.

ip dhcp arp-probe	Enable the ARP entry check function.
ip dhcp class	Configure a class and enter the global class configuration mode.
ip dhcp dns dynamic	Configure preferential assignment of the DNS server address obtained from an external DHCP server to clients when the device works in DHCP client or Point-to-Point Protocol over Ethernet (PPPoE) mode.
ip dhcp excluded-address	Configure excluded addresses that will not be assigned to a client by a DHCP server.
ip dhcp force-send-nak	Enable compulsory NAK reply.
ip dhcp monitor-vrrp-state	Enable Virtual Router Redundancy Protocol (VRRP) monitoring to ensure that a DHCP server processes request packets of DHCP clients only from the VRRP interface in Master state.
ip dhcp ping packets	Configure the number of times that a DHCP server pings a conflicted IP address.
ip dhcp ping timeout	Configure the timeout time of a ping operation for detecting address conflicts.
ip dhcp pool	Create a DHCP address pool and enter the DHCP address pool configuration mode.
ip dhcp refresh arp	Refresh trusted ARP entries.
ip dhcp relay check server-id	Enable the Server-ID check function so that a DHCP relay agent forwards DHCP request packets only to the DHCP server specified by the Server-ID field.
ip dhcp relay force-send-reply-pack	Enable the function of forcing a DHCP relay agent to send a reply packet.
ip dhcp relay information option82	Enable DHCP Option 82.
ip dhcp relay information option82 user-defined circuit-id	Customize the Circuit ID sub-option in DHCP Option 82.
ip dhcp relay information option82 user-defined remote-id	Customize the Remote ID sub-option in DHCP Option 82.
ip dhcp relay information option82 user-defined mac-format	Configure the format of the MAC address string in a sub-option of DHCP Option 82.
ip dhcp relay multiple-giaddr	Enable the function of configuring multiple gateway IP addresses on a DHCP relay agent.

ip dhcp relay suppression	Enable DHCP relay suppression.
ip dhcp relay source	Configure the source address of DHCP relay packets.
ip dhcp save-history-enable	Enable the function of saving historical leases to the database.
ip dhcp server arp-detect	Enable go-offline detection.
ip dhcp server detect	Enable rogue server detection.
ip dhcp smart-relay	Enable the automatic gateway switchover function.
ip dhcp use class	Enable address assignment based on class rules.
ip helper-address	Configure a DHCP server IP address globally or on an interface of a DHCP relay agent.
lease	Configure the lease time of an IP address assigned by a DHCP server to a DHCP client.
lease-threshold	Configure an alarm threshold for a DHCP address pool.
match ip	Configure an AM rule.
match ip default	Configure the default AM rule.
match ip loose	Enable the loose mode for AM rules.
netbios-name-server	Configure the NetBIOS Windows Internet Name Service (WINS) server that a DHCP server assigns to a DHCP client.
netbios-node-type	Configure the NetBIOS node type that a DHCP server assigns to a DHCP client.
network	Configure the primary network segment for dynamic assignment in a DHCP address pool.
next-server	Configure the boot server list that a DHCP server assigns to a DHCP client.
option	Define DHCP server options.
pool-status	Configure whether to enable a DHCP address pool.
relay agent information	Enter the Option 82 matching information configuration mode from the global class configuration mode.
relay-information hex	Configure Option 82 matching information.

remark	Configure identification information of a class.
service dhcp	Enable the DHCP Server or DHCP Relay function.
show ip dhcp binding	Display DHCP address binding information.
show ip dhcp conflict	Display IP address conflict records of a DHCP server.
show ip dhcp database	Display the running status of the database backup function of a DHCP server.
show ip dhcp dns dynamic	Display the DNS server address obtained from an external DHCP server when the device works in PPPoE or DHCP client mode.
show ip dhcp history	Display historical lease records.
show ip dhcp identifier	Display the address pool ID and address usage of a DHCP server.
show ip dhcp pool	Display the address pool status and utilization of a DHCP server.
show ip dhcp relay-statistics	Display statistics of a DHCP relay agent.
show ip dhcp server detect	Display the list of detected rogue servers.
show ip dhcp server statistics	Display statistics of a DHCP server.
show ip dhcp socket	Display the socket index used by a DHCP server.
update arp	Enable a DHCP server to add trusted ARP entries during address assignment.

1.1 address range

Function

Run the **address range** command to configure the network segment of a class.

Run the **no** form of this command to remove this configuration.

The default network segment of a class is the network segment of an address pool.

Syntax

address range *low-ip-address high-ip-address*

no address range

Parameter Description

low-ip-address: Start address of a network segment.

high-ip-address: End address of a network segment.

Command Modes

Address pool class configuration mode

Usage Guidelines

This command is configured on a Dynamic Host Configuration Protocol (DHCP) server.

Each class corresponds to one network segment. Network segments are assigned in ascending order, and the network segments of multiple classes can overlap. If a class is associated with an address pool but no network segment is configured for the class, the default network segment of the class is the same as the network segment of the address pool.

Examples

The following example sets the network segment of class 1 associated with DHCP address pool mypool0 to 172.16.1.1 to 172.16.1.8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# class class1
Hostname(config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip dhcp pool**

1.2 address-manage

Function

Run the **address-manage** command to enter the AM rule configuration mode.

Syntax

address-manage

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server in super virtual local area network (VLAN) scenarios.

Examples

The following example enters the AM rule configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-manage
Hostname(config-address-manage)#
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.3 bootfile

Function

Run the **bootfile** command to configure the boot image file name that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No boot image file name is configured by default.

Syntax

bootfile *file-name*

no bootfile

default bootfile

Parameter Description

file-name: Boot image file name.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Some DHCP clients need to download the operating system or configuration file in the boot process. A DHCP server must provide the image file name required during boot for the DHCP clients to download the file from the corresponding server, such as the Trivial File Transfer Protocol (TFTP) server. The **next-server** command is used to define the servers for boot image file download.

Examples

The following example sets the boot image file name assigned to DHCP clients with IP addresses from DHCP address pool mypool0 to **router.conf**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# bootfile router.conf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 class

Function

Run the **class** command to configure the class associated with a DHCP address pool.

Run the **no** form of this command to remove this configuration.

No class is associated with a DHCP address pool by default.

Syntax

class *class-name*

no class *class-name*

Parameter Description

class-name: Class name. The value is a case-sensitive string of 1 to 64 characters.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

In each DHCP address pool, Option 82 information is used to map address segments and classify them into different classes. A DHCP address pool can be associated with multiple classes. Each class corresponds to a different network segment.

During address assignment, a DHCP server first determines an available address pool based on the network segment of a client. Then, it determines the class of the client based on Option 82, and assigns an IP address from the network segment corresponding to the class. When a request packet matches multiple classes in the address pool, the DHCP server assigns an IP address from the network segments corresponding to the classes based on the class configuration sequence. If the number of assigned IP addresses of a class reaches the limit, the DHCP server assigns an IP address based on the next matching class. Each class corresponds to one network segment. Network segments are assigned in ascending order, and the network segments of multiple classes can overlap. If a class is associated with an address pool but no network segment is configured for the class, the default network segment of the class is the same as the network segment of the address pool.

Examples

The following example associates address pool mypool0 with class 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# class class1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 clear match ip

Function

Run the **clear match ip** command to clear the matching rules in AM rules.

Syntax

clear match ip [*interface-type interface-number* | **loose**]

Parameter Description

interface-type interface-number: Interface type and interface number.

loose: Specifies the loose mode for AM rules.

Command Modes

AM rule configuration mode

Default Level

14

Usage Guidelines

If the loose mode is configured, clients that match no AM rule can obtain IP addresses in the way same as the case with no AM rule configured.

Examples

The following example clears all matching rules in AM rules.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-manage
Hostname(config-address-manage)# clear match ip
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.6 clear ip dhcp binding

Function

Run the **clear ip dhcp binding** command to clear the DHCP IP address binding table.

Syntax

clear ip dhcp binding { * | *ip-address* }

Parameter Description

*: Clears all DHCP IP address binding records.

ip-address: IP address for which binding records are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command can clear records of automatically bound IP addresses only. To clear records of manually bound IP addresses, run the **no ip dhcp pool** command.

Examples

The following example clears the DHCP binding table of IP address 192.168.12.100.

```
Hostname> enable
Hostname# clear ip dhcp binding 192.168.12.100
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.7 clear ip dhcp conflict

Function

Run the **clear ip dhcp conflict** command to clear DHCP address conflict records.

Syntax

clear ip dhcp conflict { * | *ip-address* }

Parameter Description

*: Clears all DHCP address conflict records.

ip-address: IP address for which conflict records are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

A DHCP server uses the ping mechanism to detect address conflicts, and a DHCP client uses free Address Resolution Protocol (ARP) packets to detect address conflicts.

Examples

The following example clears all DHCP address conflict records.

```
Hostname> enable
Hostname# clear ip dhcp conflict *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.8 clear ip dhcp history

Function

Run the **clear ip dhcp history** command to clear historical DHCP address records.

Syntax

clear ip dhcp history { * | *mac-address* }

Parameter Description

*: Clears all historical DHCP address records.

mac-address: MAC address for which historical DHCP address records are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

A DHCP server saves information about all assigned IP addresses. This command is used to clear all historical address records.

Examples

The following example clears all historical DHCP address records.

```
Hostname> enable
Hostname# clear ip dhcp history *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 clear ip dhcp server detect

Function

Run the **clear ip dhcp server detect** command to clear rogue DHCP server detection records.

Syntax

clear ip dhcp server detect { * | *ip-address* }

Parameter Description

*: Clears all rogue DHCP server detection records.

ip-address: IP address for which rogue server detection records are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

A DHCP server saves addresses of detected rogue servers. This command is used to clear rogue server detection records.

Examples

The following example clears all rogue DHCP server detection records.

```
Hostname> enable
Hostname# clear ip dhcp server detect *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 clear ip dhcp server rate

Function

Run the **clear ip dhcp server rate** command to clear statistics about the processing rate of DHCP server packets on related modules.

Syntax

clear ip dhcp server rate

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command is used to clear statistics about the processing rate of DHCP server packets on different modules, such as ARP, hot backup, LSM, and socket.

Examples

The following example clears statistics about the processing rate of DHCP server packets on related modules.

```
Hostname> enable
Hostname# clear ip dhcp server rate
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 clear ip dhcp server statistics

Function

Run the **clear ip dhcp server statistics** command to clear statistics of a DHCP server.

Syntax

clear ip dhcp server statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Statistics of a DHCP server include the numbers of DHCP address pools, manually and automatically bound IP addresses, expired bindings, and sent and received packets of different types. This command is used to clear historical records and start new statistics collection.

Examples

The following example clears statistics of a DHCP server.

```
Hostname> enable
Hostname# clear ip dhcp server statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 clear ip dhcp relay statistics

Function

Run the **clear ip dhcp relay statistics** command to clear statistics of a DHCP relay agent.

Syntax

clear ip dhcp relay statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

Statistics of a DHCP relay agent include the numbers of sent and received packets of different types. This command is used to clear historical records and start new statistics collection.

Examples

The following example clears statistics of a DHCP relay agent.

```
Hostname> enable
Hostname# clear ip dhcp relay statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 client-identifier

Function

Run the **client-identifier** command to configure a unique DHCP client ID.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DHCP client ID is configured by default.

Syntax

client-identifier [*unique-identifier*]

no client-identifier

default client-identifier

Parameter Description

unique-identifier: ID of a DHCP client, in hexadecimal notation with characters separated by dots (.), for example, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Some DHCP clients use an ID instead of a hardware address to apply for an IP address from a DHCP server. A client ID consists of the media type, Media Access Control (MAC) address, and interface name. For example, if the MAC address is 00d0.f822.33b4 and interface name is GigabitEthernet 0/1, the client identifier is

0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31. **01** indicates Ethernet, and

67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hexadecimal code of GigabitEthernet 0/1. For details about media codes, see "Address Resolution Protocol Parameters" in RFC 1700.

This command can be used only when IP addresses are statically configured.

Examples

The following example configures the ID of an Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 client-name

Function

Run the **client-name** command to configure a DHCP client name.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DHCP client name is configured by default.

Syntax

client-name *client-name*
no client-name
default client-name

Parameter Description

client-name: Name of a DHCP client. A client name can use any standard American Standard Code for Information Interchange (ASCII) character set. A client name should not contain the domain name. For example, a DHCP client name can be set to **river** but cannot be set to **river.i-net.com.cn**.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command can be used only when IP addresses are manually bound. A client name should not contain the domain name.

Examples

The following example sets the name of a client with an IP address from DHCP address pool mypool0 to **river**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# client-name river
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 default-router

Function

Run the **default-router** command to configure the default gateway that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No default gateway is configured by default.

Syntax

default-router *ip-address*&<1-8>

no default-router

default default-router

Parameter Description

ip-address&<1-8>: Gateway IP address of a DHCP client. **<1-8>** indicates that up to eight gateway IP addresses can be entered, and the IP addresses are separated by spaces.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Generally, a DHCP client needs to obtain the default gateway information from a DHCP server. The DHCP server must specify at least one gateway IP address for a DHCP client, and the gateway IP address must be in the same network segment as the address assigned to the client.

Examples

The following example sets the default gateway for DHCP clients with IP addresses from DHCP address pool mypool0 to **192.168.12.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# default-router 192.168.12.1
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# default-router 225.2.2.2
```

```
% Error: ip address (225.2.2.2) is not valid!
```

Common Errors

- Non-unicast addresses are configured.
- More than eight valid addresses are configured.

Platform Description

N/A

Related Commands

N/A

1.16 dns-server

Function

Run the **dns-server** command to configure the Domain Name System (DNS) server that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DNS server is configured by default.

Syntax

dns-server *ip-address&*<1-8>

no dns-server

default dns-server

Parameter Description

ip-address&<1-8>: IP address of a DNS server. **<1-8>** indicates that up to eight DNS server IP addresses can be entered, and the IP addresses are separated by spaces.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When multiple DNS servers are defined, the first defined DNS server has the highest priority. A DHCP client selects the next DNS server only when it fails to communicate with the first defined DNS server.

When the device also serves as a DHCP client, it can transfer the obtained DNS server information to another DHCP client.

Examples

The following example sets the DNS server IP address for DHCP clients with addresses from DHCP address pool mypool0 to **192.168.12.3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# dns-server 192.168.12.3
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# dns-server 225.2.2.2
% Error: ip address (225.2.2.2) is not valid!
```

Common Errors

- Non-unicast addresses are configured.
- More than eight valid addresses are configured.

Related Commands

N/A

1.17 domain-name

Function

Run the **domain-name** command to configure the domain name that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No domain name is configured by default.

Syntax

domain-name *domain-name*

no domain-name

default domain-name

Parameter Description

domain-name: Domain name of a DHCP client.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

After a DHCP client obtains a specified domain name, it can directly use its host name to access a host whose name contains the same domain name.

Examples

The following example sets the domain name assigned to DHCP clients with addresses from DHCP address pool mypool0 to **i-net.com.cn**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# domain-name i-net.com.cn
```

Notifications

When a domain name is configured for a DHCP client, the following notification will be displayed:

```
Hostname(dhcp-config)# domain-name Hostname.com.cn
```

Common Errors

N/A

Related Commands

N/A

1.18 force-no-router

Function

Run the **force-no-router** command to forcibly disable gateway assignment to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A DHCP server assigns a gateway to a DHCP client by default.

Syntax

force-no-router

no force-no-router

default force-no-router

Parameter Description

N/A

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Examples

The following example forcibly disable gateway assignment to DHCP clients with addresses from DHCP address pool mypool0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# force-no-router
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.19 hardware-address

Function

Run the **hardware-address** command to configure a hardware address for a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DHCP client hardware address is configured by default.

Syntax

hardware-address *hardware-address* [*type*]

no hardware-address

default hardware-address

Parameter Description

hardware-address: MAC address of a DHCP client.

type: Hardware platform protocol of a DHCP client. The value can be a character string or number. Character string options include **ethernet** and **ieee802**. Number options include **1** (10M Ethernet) and **6** (IEEE 802). If no option is defined, the default option is **ethernet**.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command can be used only when IP addresses are manually bound.

Examples

The following example sets the MAC address of a DHCP client with an address from DHCP address pool mypool0 to **00d0.f838.bf3d**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# hardware-address 00d0.f838.bf3d
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.20 host

Function

Run the **host** command to configure the IP address and network mask of a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IP address or network mask is configured for a DHCP client by default.

Syntax

host *ip-address* [*netmask*]

no host

default host

Parameter Description

ip-address: IP address of a DHCP client host.

netmask: Network mask of a DHCP client host.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

If no network mask is defined, the DHCP server uses the natural mask of the IP address as the network mask. The natural mask is 255.0.0.0 for class A addresses, 255.255.0 for class B addresses, and 255.255.255.0 for class C addresses.

This command can be used only when IP addresses are manually bound.

Examples

The following example sets the IP address and network mask of a DHCP client with an address from DHCP address pool mypool0 to **192.168.12.91** and **255.255.255.240**, respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# host 192.168.12.91 255.255.255.240
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# host 225.2.2.2 255.0.0.0
% Error: ip address 225.2.2.2 is not valid!
```

Common Errors

- An invalid address is configured.

Related Commands

N/A

1.21 ip dhcp arp-probe

Function

Run the **ip dhcp arp-probe** command to enable the ARP entry check function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ARP entry check function is disabled by default.

Syntax

ip dhcp arp-probe

no ip dhcp arp-probe

default ip dhcp arp-probe

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The ARP entry check function can be used with the ping mechanism to detect IP address conflicts and prevent IP address conflicts with clients configured with static IP addresses. If a client configured with a static IP address exists and L2 isolation is configured in an environment and the ping mechanism for IP address conflict detection becomes invalid (for example, a firewall is enabled on the client), this IP address may be assigned to another client that dynamically applies for an address, resulting in an IP address conflict.

The ARP entry check function can be enabled only in the preceding scenario. If ARP attacks exist, this function cannot be enabled. Otherwise, the DHCP address assignment service is affected. As a result, it takes a long time for a client to apply for an IP address or a client cannot apply for an IP address.

Examples

The following example enables the ARP entry check function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp arp-probe
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip dhcp class

Function

Run the **ip dhcp class** command to configure a class and enter the global class configuration mode.

Run the **no** form of this command to remove this configuration.

No class is configured by default.

Syntax

ip dhcp class *class-name*

no ip dhcp class *class-name*

Parameter Description

class-name: Class name. The value is a case-sensitive string of 1 to 64 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

After this command is executed, the system enters the global class configuration mode. In this configuration mode, you can configure Option 82 and the identifier of a class.

Examples

The following example configures a global class named **myclass** and enters the global class configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ip dhcp dns dynamic

Function

Run the **ip dhcp dns dynamic** command to configure preferential assignment of the DNS server address obtained from an external DHCP server to clients when the device works in DHCP client or Point-to-Point Protocol over Ethernet (PPPoE) mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Preferential assignment of the DNS server address obtained from an external DHCP server is not configured by default.

Syntax

ip dhcp dns dynamic

no ip dhcp dns dynamic

default ip dhcp dns dynamic

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When the device works in PPPoE or DHCP client mode, a DNS server address can be automatically obtained from an external DHCP server and be configured on the DHCP server of the local device, so that users do not need to perform DNS configuration. When the device serves as a DHCP server, it preferentially assigns clients with the DNS server address obtained from the external DHCP server.

Examples

The following example preferentially assigns the DNS server address obtained from an external DHCP server to clients when the device works in PPPoE or DHCP client mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp dns dynamic
```

Notifications

N/A

Common Errors

When the device works in PPPoE or DHCP client mode, it does not obtain a DNS server address from an external DHCP server.

Platform Description

N/A

Related Commands

N/A

1.24 ip dhcp excluded-address

Function

Run the **ip dhcp excluded-address** command to configure excluded addresses that will not be assigned to a client by a DHCP server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No excluded IP address is configured by default. A DHCP server assigns all addresses from an IP address pool to DHCP clients.

Syntax

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

default ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

Parameter Description

low-ip-address: Excluded IP address or the start IP address of an excluded IP address range.

high-ip-address: End address of an excluded IP address range. The default value is the address defined by the *low-ip-address* parameter.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

If no excluded IP address is configured, a DHCP server assigns all IP addresses from an IP address pool to DHCP clients. This command is used to reserve some IP addresses for specific hosts and prevent these addresses being assigned to other DHCP clients. Excluded IP addresses help a DHCP server shorten the time for detecting IP address conflicts during address assignment.

Examples

The following example sets an excluded address range to 192.168.12.100 to 192.168.12.150.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Notifications

When an invalid excluded address is configured, the following notification will be displayed:

```
Hostname(config)# ip dh excluded-address 225.1.1.1
% Error: Ip address 225.1.1.1 or 225.1.1.1 is not valid!
```

When a non-existent excluded address is deleted, the following notification will be displayed:

```
Hostname(config)# no ip dhcp excluded-address 20.1.1.1
% Range [20.1.1.1, 20.1.1.1] is not in the database.
```

Common Errors

- An invalid excluded address is configured.
- A non-existent excluded address is deleted.

Platform Description

N/A

Related Commands

N/A

1.25 ip dhcp force-send-nak

Function

Run the **ip dhcp force-send-nak** command to enable compulsory NAK reply.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Compulsory NAK reply is enabled by default.

Syntax

ip dhcp force-send-nak

no ip dhcp force-send-nak

default ip dhcp force-send-nak

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

A DHCP client preferentially applies for the previously used IP address after a restart. The DHCP client sends a DHCP REQUEST packet to renew the IP address lease. If the IP address is unavailable, the DHCP server sends an NAK packet for the client to re-send a DHCP DISCOVER packet to apply for a new IP address. If the corresponding IP address lease record does not exist on the DHCP server, the client sends DHCP REQUEST packet repeatedly until the request times out. In wireless applications, compulsory NAK reply is provided for clients to re-send DHCP DISCOVER packets to apply for IP addresses quickly.

Examples

The following example disables compulsory NAK reply.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dhcp force-send-nak
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ip dhcp monitor-vrrp-state

Function

Run the **ip dhcp monitor-vrrp-state** command to enable Virtual Router Redundancy Protocol (VRRP) monitoring to ensure that a DHCP server processes request packets of DHCP clients only from the VRRP interface in Master state.

Run the **no** form of this command to disable this feature. In this case, a DHCP server processes all DHCP request packets.

Run the **default** form of this command to restore the default configuration.

VRRP monitoring is disabled for an interface by default.

Syntax

ip dhcp monitor-vrrp-state

no ip dhcp monitor-vrrp-state

default ip dhcp monitor-vrrp-state

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command can be configured only on L3 interfaces.

For an interface configured with a VRRP address and VRRP monitoring, a DHCP server processes request packets of DHCP clients only from the interface in Master state and discards other packets. If no VRRP address is configured, the DHCP server does not monitor the VRRP status and processes all DHCP request packets.

Examples

The following example enables VRRP monitoring to ensure that a DHCP server processes request packets of DHCP clients only from the VRRP interface in Master state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip dhcp monitor-vrrp-state
```

Notifications

When VRRP monitoring is configured on an L2 interface, the following notification will be displayed:

```
Hostname(config-if-GigabitEthernet 0/2)# ip dhcp monitor-vrrp-state
% Invalid input detected at '^' marker.
```

Common Errors

- VRRP monitoring is configured on an L2 interface.

Platform Description

N/A

Related Commands

N/A

1.27 ip dhcp ping packets

Function

Run the **ip dhcp ping packets** command to configure the number of times that a DHCP server pings a conflicted IP address.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A DHCP server pings a conflicted IP address two times by default.

Syntax

ip dhcp ping packets [*ping-times*]

no ip dhcp ping packets

default ip dhcp ping packets

Parameter Description

Ping-times: Number of times that a DHCP server pings a conflicted IP address. The value range is from 0 to 10. The value **0** indicates that the ping operation is disabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When a DHCP server attempts to assign an IP address from a DHCP address pool, it uses the ping mechanism to check whether the IP address is occupied by another host. If yes, the DHCP server records the IP address. If not, the DHCP server assigns the IP address to a DHCP client.

Examples

The following example sets the number of times that a DHCP server pings a conflicted IP address to **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp ping packets 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ip dhcp ping timeout

Function

Run the **ip dhcp ping timeout** command to configure the timeout time of a ping operation for detecting address conflicts.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default timeout time of a ping operation for detecting address conflicts is 500 ms.

Syntax

ip dhcp ping timeout *time*

no ip dhcp ping timeout

default ip dhcp ping timeout

Parameter Description

time: Duration that a DHCP server waits for a ping operation response, in milliseconds. The value range is from 100 to 10000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Examples

The following example sets the timeout time of a ping operation for detecting address conflicts to 600 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp ping timeout 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ip dhcp pool

Function

Run the **ip dhcp pool** command to create a DHCP address pool and enter the DHCP address pool configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DHCP address pool is configured by default.

Syntax

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

default ip dhcp pool *pool-name*

Parameter Description

pool-name: Address pool name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command is used to enter the DHCP address pool configuration mode. In DHCP address pool configuration mode, you can configure the IP address range, DNS server address, and default gateway.

Examples

The following example creates a DHCP address pool named **mypool0** and enters the DHCP address pool configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip dhcp pool**

1.30 ip dhcp refresh arp

Function

Run the **ip dhcp refresh arp** command to refresh trusted ARP entries.

Syntax

ip dhcp refresh arp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

After this command is executed, a DHCP server refreshes trusted ARP entries only for clients assigned with addresses from an address pool that has the **update arp** command configured.

Examples

The following example refreshes trusted ARP entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp refresh arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 ip dhcp relay check server-id

Function

Run the **ip dhcp relay check server-id** command to enable the **Server-ID** check function so that a DHCP relay agent forwards DHCP request packets only to the DHCP server specified by the **Server-ID** field.

Run the **no** form of this command to disable this feature.

The **Server-ID** check function is disabled by default.

Syntax

ip dhcp relay check server-id

no ip dhcp relay check server-id

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

In a DHCP relay application environment, multiple DHCP servers are configured for each network device to provide server backup, thereby ensuring normal network operation. When a DHCP client has selected a DHCP server to send a DHCP REQUEST packet, a **Server-ID** option is carried in the packet. To reduce server load in specific environments, enable the **Server-ID** check function on the DHCP relay agent, so as to send the DHCP REQUEST packet to a DHCP server specified in this option.

In this case, the DHCP relay agent sends DHCP request packets only to the specified server. If this function is not configured, the DHCP relay agent sends DHCP request packets to all configured DHCP servers.

Examples

The following example enables the **Server-ID** check function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay check server-id
```

The following example disables the **Server-ID** check function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dhcp relay check server-id
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 ip dhcp relay force-send-reply-pack

Function

Run the **ip dhcp relay force-send-reply-pack** command to enable the function of forcing a DHCP relay agent to send a reply packet.

Run the **no** form of this command to disable this feature.

The function of forcing a DHCP relay agent to send a reply packet is disabled by default.

Syntax

ip dhcp relay force-send-reply-pack

no ip dhcp relay force-send-reply-pack

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

After the function of forcing a DHCP relay agent to send a reply packet is enabled, a DHCP relay agent forcibly specifies a gateway interface to send a reply packet if it fails to find a MAC address egress. When this command is not configured, the DHCP relay agent discards packets if it fails to find a MAC address egress.

Examples

The following example enables the function of forcing a DHCP relay agent to send a reply packet.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay force-send-reply-pack
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 ip dhcp relay information option82

Function

Run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Run the **no** form of this command to disable this feature.

DHCP Option 82 is disabled by default.

Syntax

ip dhcp relay information option82

no ip dhcp relay information option82

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

When this function is enabled and the device serves as a DHCP relay agent, the device adds Option 82 to a DHCP request packet to be forwarded to a DHCP server. The encapsulation format of **Circuit ID** is "slot(1):port(1):dev_name(<=64)" and that of Remote ID is "user_mac(6):iftype(1):port_name(<=64):vid(2)".

Examples

The following example enables DHCP Option 82.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay information option82
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 ip dhcp relay information option82 user-defined circuit-id

Function

Run the **ip dhcp relay information option82 user-defined circuit-id** command to customize the **Circuit ID** sub-option in DHCP Option 82.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Customization of **Circuit ID** in DHCP Option 82 is disabled by default.

Syntax

ip dhcp relay information option82 user-defined circuit-id *circuit-id-text*

no ip dhcp relay information option82 user-defined circuit-id

default ip dhcp relay information option82 user-defined circuit-id

Parameter Description

circuit-id-text: User-defined **Circuit ID** content. The value is a case-sensitive string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in user-defined mode, this command is used to customize **Circuit ID** in Option 82.

When defining the format of Option 82, you can use the keywords described in the following table. The format string behind the keywords can be set to the hexadecimal encapsulation format, ASCII encapsulation format, or hexadecimal and ASCII hybrid encapsulation format.

Table 1-1 Circuit ID Format String

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
hostname	Host name	√	×	-	Example: Hostname
devicename	Device model	√	×	-	Example: S5750C-48GT4XS-H
portname	Interface name	√	×	-	Example: GigabitEthernet 0/1
portsname	Interface name abbreviation	√	×	-	Example: Te0/2.5
porttype	Interface type	√	√	1 B	Example: ● When ASCII is used to represent 1, the padding value is **0x31**. ● When hexadecimal is used to represent 1, the padding value is **0x01**.
sysmac	Interface MAC address	√	√	6 B	Example: ● ASCII: 2222.2222.2222 ● Hexadecimal: 0x22 0x22 0x22 0x22 0x22 0x22
slot	Slot ID	√	√	1 B	Example: ● When ASCII is used to represent 0, the padding value is **0x30**. ● When hexadecimal is used to represent 0, he padding value is **0x00**.

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
port	Port number	√	√	1 B	Example: ● When ASCII is used to represent 2, the padding value is **0x32**. ● When hexadecimal is used to represent 2, the padding value is **0x02**.
subport	Sub-port number	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
svlan	Outer VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
cvlan	Inner VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					used to represent 5, the padding value is **0x0005**.
length	Length of content following the length keyword	×	√	1 B	Example: When hexadecimal is used to represent 5, the padding value is **0x05**.

Note: √ indicates that a keyword supports the corresponding encapsulation format, × indicates that a keyword does not support the corresponding encapsulation format, and - indicates meaningless.

Special characters are described as follows:

- % followed by keywords defined above indicates the format of the keywords. When the percent symbol (%) needs to be contained in the input string, enter %%, which will be converted into a single common percent symbol (%) during parsing.
- The backslash (\) indicates an escape character, and the special character following the backslash (\) indicates the special character itself. For example, \\ indicates the backslash (\) and \" indicates the quotation mark (").
- The double quotation marks ("") indicate that data enclosed is encapsulated in string format. Data without or outside the double quotation marks is encapsulated in hexadecimal format.
- Strings in ASCII format can contain 0 to 9, a to z, A to Z, and the following symbols: !, @, #, $, %, ^, &, *, (), _, +, |, -, =, \, [], {}, ;, :, '", /, ?, ., ,, <>, `.
- For characters %\" in ASCII format, add the prefix (\) in front of the characters. In ASCII format, only keywords and several specific symbols are converted and other data remains unchanged.
- If there is no escape character '\' in front of '%' in configuration commands, the key value in the information field must be added behind. Otherwise, the configuration is incorrect and an error is prompted. If the character '\' needs to be configured, enter "\\".
- For strings in hexadecimal format, digits are encapsulated into Option 82 directly in hexadecimal notation. When hexadecimal data is used, strings begin with 0X or 0x. When the number of valid characters in the hexadecimal data is an odd, add one 0 to the frontmost. When decimal data is used, the data ranges from 0 to 255 and occupies one byte. You can use spaces to enter multiple pieces of decimal data consecutively.
- Blank characters in hexadecimal notation are ignored.
- If the user-defined mode is configured but no corresponding user-defined format is configured, each sub-option of Option 82 is padded in standard mode.

Examples

The following example sets the content of **Circuit ID** in Option 82 to *host name-interface name*.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay information option82 user-defined circuit-id
"%hostname-%portname"
```

Notifications

N/A

Common Errors

The user-defined string does not meet configuration requirements.

Platform Description

N/A

Related Commands

N/A

1.35 ip dhcp relay information option82 user-defined remote-id

Function

Run the **ip dhcp relay information option82 user-defined remote-id** command to customize the **Remote ID** sub-option in DHCP Option 82.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No custom information is configured for **Remote ID** of DHCP Option 82 by default.

Syntax

ip dhcp relay information option82 user-defined remote-id *remote-id-text*

no ip dhcp relay information option82 user-defined remote-id

default ip dhcp relay information option82 user-defined remote-id

Parameter Description

remote-id-text: User-defined **Remote ID** content. The value is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in user-defined mode, this command is used to customize **Remote ID** in Option 82.

When defining the format of Option 82, you can use the keywords described in the following table. The format string behind the keywords can be set to the hexadecimal encapsulation format, ASCII encapsulation format, or hexadecimal and ASCII hybrid encapsulation format.

Table 1-2 Remote ID Format String

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
hostname	Host name	√	×	-	Example: Hostname
devicename	Device model	√	×	-	Example: S5750C-48GT4XS-H
portname	Interface name	√	×	-	Example: GigabitEthernet 0/1
portsname	Interface name abbreviation	√	×	-	Example: Te0/2.5
porttype	Interface type	√	√	1 B	Example: ● When ASCII is used to represent 1, the padding value is **0x31**. ● When hexadecimal is used to represent 1, the padding value is **0x01**.
sysmac	Interface MAC address	√	√	6 B	Example: ● ASCII: 2222.2222.2222 ● Hexadecimal: 0x22 0x22 0x22 0x22 0x22 0x22
slot	Slot ID	√	√	1 B	Example: ● When ASCII is used to represent 0, the padding value is **0x30**. ● When hexadecimal is used to

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					represent 0, he padding value is **0x00**.
port	Port number	√	√	1 B	Example: ● When ASCII is used to represent 2, the padding value is **0x32**. ● Hexadecimal: 2. The padding value is **0x02**.
subport	Sub-port number	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
svlan	Outer VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
cvlan	Inner VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**.

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					• When hexadecimal is used to represent 5, the padding value is **0x0005**.
length	Length of content following the length keyword	×	√	1 B	Example: When hexadecimal is used to represent 5, the padding value is **0x05**.

Note: √ indicates that a keyword supports the corresponding encapsulation format, × indicates that a keyword does not support the corresponding encapsulation format, and - indicates meaningless.

Special characters are described as follows:

- % followed by keywords defined above indicates the format of the keywords. When the percent symbol (%) needs to be contained in the input string, enter %%, which will be converted into a single common percent symbol (%) during parsing.
- The backslash (\) indicates an escape character, and the special character following the backslash (\) indicates the special character itself. For example, \\ indicates the backslash (\) and \" indicates the quotation mark (").
- The double quotation marks ("") indicate that data enclosed is encapsulated in string format. Data without or outside the double quotation marks is encapsulated in hexadecimal format.
- Strings in ASCII format can contain 0 to 9, a to z, A to Z, and the following symbols: !, @, #, $, %, ^, &, *, (), _, +, |, -, =, \, [], {}, ;, :, '", /, ?, ., ,, <>, `.
- For characters %\" in ASCII format, add the prefix (\) in front of the characters. In ASCII format, only keywords and several specific symbols are converted and other data remains unchanged.
- If there is no escape character '%' in front of '%' in configuration commands, the key value in the information field must be added behind. Otherwise, the configuration is incorrect and an error is prompted. If the character '\' needs to be configured, enter "\\".
- For strings in hexadecimal format, digits are encapsulated into Option 82 directly in hexadecimal notation. When hexadecimal data is used, strings begin with 0X or 0x. When the number of valid characters in the hexadecimal data is an odd, add one 0 to the frontmost. When decimal data is used, the data ranges from 0 to 255 and occupies one byte. You can use spaces to enter multiple pieces of decimal data consecutively.
- Blank characters in hexadecimal notation are ignored.
- If the user-defined mode is configured but no corresponding user-defined format is configured, each sub-option of Option 82 is padded in standard mode.

Examples

The following example sets the content of **Remote ID** in Option 82 to *host name-interface name*.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay information option82 user-defined remote-id
"%hostname-%portname"
```

Notifications

N/A

Common Errors

The user-defined string does not meet configuration requirements.

Platform Description

N/A

Related Commands

N/A

1.36 ip dhcp relay information option82 user-defined mac-format

Function

Run the **ip dhcp relay information option82 user-defined mac-format** command to configure the format of the MAC address string in a sub-option of DHCP Option 82.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default MAC address format is H.H.H.

Syntax

ip dhcp relay information option82 user-defined mac-format *mac-format-type*

no ip dhcp relay information option82 user-defined mac-format

default ip dhcp relay information option82 user-defined mac-format

Parameter Description

mac-format-type: Format of the MAC address string in user-defined mode. The value range is from 0 to 2, and the default value is **0**. **0** indicates the H.H.H format, **1** indicates the H-H-H format, and **2** indicates the H:H:H:H:H:H format.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in user-defined mode, this command is used to convert keyword **%sysmac** in ASCII encapsulation format in a sub-option of Option 82 to a MAC address string in corresponding format.

Examples

The following example sets the format of the MAC address string in a sub-option of DHCP Option 82 to H-H-H.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay information option82 user-defined mac-format 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 ip dhcp relay multiple-giaddr

Function

Run the **ip dhcp relay multiple-giaddr** command to enable the function of configuring multiple gateway IP addresses on a DHCP relay agent.

Run the **no** form of this command to disable this feature.

The function of configuring multiple gateway IP addresses on a DHCP relay agent is disabled by default.

Syntax

ip dhcp relay multiple-giaddr

no ip dhcp relay multiple-giaddr

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

After the function of configuring multiple gateway IP addresses is enabled, a DHCP relay agent can use multiple interface IP addresses to send address applications to a DHCP server. Generally, the primary IP address is used as the gateway IP address, and the DHCP server assigns a network segment based on the gateway IP address. When a client fails to apply for an IP address over the gateway by using the primary IP address, it applies for an IP address over the gateway by using a secondary IP address.

After the automatic gateway switchover function is enabled, the DHCP relay agent adds another address to the **giaddr** field if it does to receive a reply packet for three consecutive DISCOVER packets.

Examples

The following example enables the function of configuring multiple gateway IP addresses on a DHCP relay agent.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp relay multiple-giaddr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 ip dhcp relay suppression

Function

Run the **ip dhcp relay suppression** command to enable DHCP relay suppression.

Run the **no** form of this command to disable this feature.

DHCP relay suppression is disabled on all interfaces by default.

Syntax

no ip dhcp relay suppression

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

After you configure this command on an interface, DHCP request packets received over the interface are filtered out, but the other DHCP requests are forwarded.

Examples

The following example enables DHCP relay suppression on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 ip dhcp relay source

Function

Run the **ip dhcp relay source** command to configure the source address of DHCP relay packets.

Run the **no** form of this command to remove this configuration.

No source address is configured for DHCP relay packets by default.

Syntax

ip dhcp relay source *ip-address*

no ip dhcp relay source

Parameter Description

ip-address: Source address of DHCP relay packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

In some networks, multiple DHCP relay agents use the same interface IP address. In this case, you need to run this command on the DHCP relay agent to add another interface IP address to the source address field and **Giaddr** field of DHCP relay packets. Only one source IP address can be specified for DHCP relay packets on an interface.

Examples

The following example configures the source address of DHCP relay packets on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp relay source 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 ip dhcp save-history-enable

Function

Run the **ip dhcp save-history-enable** command to enable the function of saving historical leases to the database.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of saving historical leases to the database is disabled by default.

Syntax

ip dhcp save-history-enable

no ip dhcp save-history-enable

default ip dhcp save-history-enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

N/A

Usage Guidelines

This command is configured on a DHCP server.

With this function enabled, after a DHCP server assigns an IP address to a client and the client goes offline, the DHCP server saves the IP address lease of the client to the database. When the client goes online again, the DHCP server assigns this address to the client again. Historical leases are saved when a DHCP process restarts or the device performs a hot backup switchover.

Examples

The following example enables the function of saving historical leases to the database.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp save-history-enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 ip dhcp server arp-detect

Function

Run the **ip dhcp server arp-detect** command to enable go-offline detection.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Go-offline detection is disabled by default.

Syntax

ip dhcp server arp-detect

no ip dhcp server arp-detect

default ip dhcp server arp-detect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Go-offline detection enables a DHCP server to check whether a client is offline. If a user goes offline and does not go online again within a period of time, the DHCP server reclaims the IP address assigned to the user.

Examples

The following example enables go-offline detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp server arp-detect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 ip dhcp server detect

Function

Run the **ip dhcp server detect** command to enable rogue server detection.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Rogue server detection is disabled by default.

Syntax

ip dhcp server detect

no ip dhcp server detect

default ip dhcp server detect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

After rogue server detection is configured, rogue servers in a network are recorded into logs.

Examples

The following example enables rogue server detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp server detect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 ip dhcp smart-relay

Function

Run the **ip dhcp smart-relay** command to enable the automatic gateway switchover function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The automatic gateway switchover function is disabled by default.

Syntax

ip dhcp smart-relay

no ip dhcp smart-relay

default ip dhcp smart-relay

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

After the function of configuring multiple gateway IP addresses on a DHCP relay agent is enabled, the primary IP address is used as the gateway IP address and the DHCP server assigns a network segment based on the gateway IP address. When a client fails to apply for an IP address over the gateway by using the primary IP address, it applies for an IP address over the gateway by using a secondary IP address after 24s.

After the automatic gateway switchover function is enabled, the DHCP relay agent adds another address to the **giaddr** field if it does not receive a reply packet for three consecutive DISCOVER packets. The relay gateway address switching sequence starts from the primary IP address to secondary IP addresses (secondary IP addresses are traversed based on their configuration sequence) until an IP address is obtained successfully.

Examples

The following example enables the automatic gateway switchover function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp smart-relay
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 ip dhcp use class

Function

Run the **ip dhcp use class** command to enable address assignment based on class rules.

Run the **no** form of this command to disable this feature.

Address assignment based on class rules is disabled by default.

Syntax

ip dhcp use class

no ip dhcp use class

Parameter Description

N/A

Command Modes

Global configuration mode

Usage Guidelines

This command is configured on a DHCP server.

When clients apply for IP addresses through different access points (APs), Option 82 carried by packets of the clients is different. Class rules are used to match Option 82 to assign clients with IP addresses in different network segments.

Examples

The following example enables address assignment based on class rules.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp use class
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 ip helper-address

Function

Run the **ip helper-address** command to configure a DHCP server IP address globally or on an interface of a DHCP relay agent.

Run the **no** form of this command to remove this configuration.

No DHCP server IP address is configured for a DHCP relay agent by default.

Syntax

ip helper-address { **cycle-mode** | [**vrf** *vrf-name*] *ip-address* }

no ip helper-address { **cycle-mode** | [**vrf** *vrf-name*] *ip-address* }

Parameter Description

cycle-mode: Forwards DHCP request packets to all DHCP servers.

vrf *vrf-name*: Specifies the virtual routing and forwarding (VRF) instance to which the specified DHCP server belongs. The default value is the VRF instance of the interface over which packets are sent.

ip-address: DHCP server IP address.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP relay agent.

After a DHCP server IP address is configured, the DHCP relay agent forwards DHCP request packets to a DHCP server and DHCP reply packets to DHCP clients.

The DHCP server address can be globally configured or configured on an L3 interface. A maximum of 20 DHCP server addresses can be globally configured or configured on each L3 interface. When an interface receives a DHCP request packet, the DHCP server list on the interface prevails over that configured globally. If the interface is not configured with the DHCP server list, the global DHCP server list takes effect.

A DHCP relay agent supports the VRF-based relay function. To configure the function, add VRF parameters before the server address.

In global configuration mode, the **cycle-mode** parameter of the DHCP relay agent can be configured. If **cycle-mode** is configured, the DHCP relay agent forwards packets from DHCP clients to all DHCP servers configured on L3 interfaces or VRFs. If **cycle-mode** is not configured, the DHCP relay agent forwards packets from DHCP clients only to the first DHCP server meeting the preceding rules. **cycle-mode** is configured only in global configuration mode but takes effect in both global and interface configuration modes. **cycle-mode** is configured by default.

Examples

The following example sets the DHCP server IP address on VLAN 1 to **192.168.11.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip helper-address 192.168.11.1
```

The following example sets the global DHCP server IP address to **192.168.100.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip helper-address 192.168.100.1
```

The following example enables a DHCP relay agent to forward DHCP request packets to all DHCP servers.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip helper-address cycle-mode
```

Notifications

N/A

Common Errors

- The **ip helper-address** command is configured on an L2 interface.
- The DHCP Relay function is disabled when the **ip helper-address** command is configured.
- A DHCP client is configured to obtain an IP address through a DHCP relay agent and directly from a DHCP server. As a result, the DHCP client fails to obtain a correct IP address.

Platform Description

N/A

Related Commands

N/A

1.46 lease

Function

Run the **lease** command to configure the lease time of an IP address assigned by a DHCP server to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default lease time is permanent for addresses in a static address pool and one day for addresses in other address pools.

Syntax

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

default lease

Parameter Description

days: Lease time, in days. The value range is from 0 to 365. The default value is **1**.

hours: Lease time, in hours. You must define days before hours. The value range is from 0 to 23. The default value is **0**.

minutes: Lease time, in minutes. You must define days and hours before minutes. The value range is from 0 to 59. The default value is **0**.

infinite: Specifies a permanent lease.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When a lease time is to expire, a DHCP client sends a request for lease renewal. Generally, a DHCP server allows lease renewal and the IP address remains unchanged. The lease time ranges from 1 minute to 365 days, 23 hours, and 59 minutes.

Examples

The following example sets the lease time of IP addresses assigned to DHCP clients from address pool mypool0 to 1 hour.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease 0 1
```

The following example sets the lease time of IP addresses assigned to DHCP clients from address pool mypool0 to 1 minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease 0 0 1
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.47 lease-threshold

Function

Run the **lease-threshold** command to configure an alarm threshold for a DHCP address pool.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default alarm threshold is 90% for the address pool.

Syntax

lease-threshold *threshold-percentage*

no lease-threshold

default lease-threshold

Parameter Description

threshold-percentage: Alarm threshold of an address pool, in percentage (%). The value range is from 60 to 100.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When the IP address usage of an address pool reaches the threshold, a DHCP server generates syslog alarms. The IP address usage is the ratio of assigned IP addresses to available IP addresses in an address pool. If the number of assigned IP addresses exceeds the alarm threshold, one alarm is generated every 5 minutes.

Examples

The following example sets the alarm threshold of DHCP address pool mypool0 to **80%**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease-threshold 80
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.48 match ip

Function

Run the **match ip** command to configure an AM rule.

Run the **no** form of this command to remove this configuration.

No AM rule is configured by default.

Syntax

match ip *ip-address mask* [*interface-type interface-number*] [**add** | **remove**] **vlan** *vlan-id*

no match ip *ip-address mask* [*interface-type interface-number*] [**add** | **remove**] **vlan** *vlan-id*

clear match ip [*interface-type interface-number*]

Parameter Description

ip-address: Network address.

mask: Address mask.

interface-type interface-number: Interface type and interface number.

add: Adds a specified VLAN.

remove: Removes a specified VLAN.

vlan *vlan-id*: Specifies the index of a VLAN.

Command Modes

AM rule configuration mode

Default Level

14

Usage Guidelines

In super VLAN scenarios, a client that meets requirements of client matching rule in a DHCP static address pool is assigned with an address from this static address pool regardless of a sub VLAN of the client. During address assignment based on AM rules, an address is assigned to the client regardless of the sub VLAN or DHCP server port from which DHCP requests are received, as long as the assigned address takes effect in the corresponding VLAN.

AM rules take effect only for static address assignment and are invalid to dynamic address assignment.

Examples

The following example configures an AM rule: For DHCP clients from GigabitEthernet 0/1 in VLAN 10, the network number is set to **192.168.11.0** and the mask is set to **255.255.255.0**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-manage
Hostname(config-address-manage)# match ip 192.168.11.0 255.255.255.0 gigabitethernet
0/1 vlan 10
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.49 match ip default

Function

Run the **match ip default** command to configure the default AM rule.

Run the **no** form of this command to remove this configuration.

No default AM rule is configured by default.

Syntax

match ip default *ip-address mask*

no match ip default *ip-address mask*

Parameter Description

ip-address: Network address.

mask: Address mask.

Command Modes

AM rule configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the DHCP server assigns an IP address from the default range to a DHCP client if no AM matching rule is configured on the interface over which the DHCP request is sent. If this command is not configured, IP addresses are assigned through the regular process.

Examples

The following example configures the default AM rule: the network number is 192.168.12.0, and the mask is 255.255.255.0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-manage
Hostname(config-address-manage)# match ip default 192.168.12.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.50 match ip loose

Function

Run the **match ip loose** command to enable the loose mode for AM rules.

Run the **no** form of this command to disable this feature.

The loose mode of AM rules is disabled by default.

Syntax

match ip loose

no match ip loose

Parameter Description

N/A

Command Modes

AM rule configuration mode

Default Level

14

Usage Guidelines

After AM rules based on VLAN or VLAN + port are configured, IP addresses within a specified range are assigned to clients that match these rules. Clients that fail to match the rules cannot obtain IP addresses. You can run the **match ip loose** command to enable the loose mode for AM rules. In this case, clients that match no AM rule can obtain IP addresses in the way same as the case with no AM rule configured.

Examples

The following example enables the loose mode for AM rules.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-manage
Hostname(config-address-manage)# match ip loose
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.51 netbios-name-server

Function

Run the **netbios-name-server** command to configure the NetBIOS Windows Internet Name Service (WINS) server that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No NetBIOS WINS server is configured by default.

Syntax

netbios-name-server *ip-address&*<1-8>

no netbios-name-server

default netbios-name-server

Parameter Description

ip-address&<1-8>: IP address of a NetBIOS WINS server. **<1-8>** indicates that up to eight NetBIOS WINS server IP addresses can be entered, and the IP addresses are separated by spaces.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When multiple NetBIOS WINS servers are defined, the first defined NetBIOS WINS server has the highest priority. A DHCP client selects the next NetBIOS WINS server only when it fails to communicate with the first defined NetBIOS WINS server.

Examples

The following example sets the NetBIOS WINS server IP address assigned to DHCP clients with addresses from DHCP address pool mypool0 to **192.168.12.3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# netbios-name-server 192.168.12.3
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# netbios-name-server 225.2.2.2
%Error: ip address (225.2.2.2) is not valid!
```

Common Errors

- Non-unicast addresses are configured.
- More than eight valid addresses are configured.

Related Commands

N/A

1.52 netbios-node-type

Function

Run the **netbios-node-type** command to configure the NetBIOS node type that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No NetBIOS node type is configured by default.

Syntax

netbios-node-type *type*

no netbios-node-type

default netbios-node-type

Parameter Description

Type: NetBIOS node type, which can be defined as:

- A hexadecimal number, ranging from 0 to FF. Only the following values are available:
  - **1**: Broadcast node
  - **2**: Peer-to-peer node
  - **4**: Mixed node
  - **8**: Hybrid node
- A character string:
  - **b-node**: Broadcast node
  - **p-node**: Peer-to-peer node
  - **m-node**: Mixed node
  - **h-node**: Hybrid node

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

NetBIOS node types for Microsoft DHCP clients include the following:

- Broadcast: Parses NetBIOS names in broadcast mode.
- Peer-to-peer: Requests the WINS server to parse NetBIOS names.
- Mixed: Requests name parsing in broadcast mode and connects to the WINS server to parse names.
- Hybrid: Requests the WINS server to parse NetBIOS names, and parses NetBIOS names in broadcast mode if no response is received.

The default node type of a DHCP client running a Microsoft operating system is broadcast or hybrid. If no WINS server is configured, the client is a broadcast node. Otherwise, it is a hybrid node. You are advised to set the NetBIOS node type to hybrid.

Examples

The following example sets the NetBIOS node type to hybrid in DHCP address pool mypool0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# netbios-node-type h-node
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.53 network

Function

Run the **Network** command to configure the primary network segment for dynamic assignment in a DHCP address pool.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No primary network segment for dynamic assignment in a DHCP address pool is configured by default.

Syntax

network *network-number mask* [*low-ip-address high-ip-address*]

no network

default network

Parameter Description

network-number: Network number of IP addresses in a DHCP address pool.

mask: Network mask of IP addresses in a DHCP address pool. If no mask is defined, the natural mask is applied.

low-ip-address: Start IP address.

high-ip-address: End IP address.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

This command is used to define a subnet and subnet mask of an address pool to provide a DHCP server with a range of addresses. Unless excluded addresses are configured, the DHCP server assigns all addresses from an address pool to DHCP clients. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address is checked until a valid address is assigned.

To display address assignment information, run the **show ip dhcp binding** command. To display address conflict detection information, run the **show ip dhcp conflict** command.

Examples

The following example sets the network number and mask of DHCP address pool mypool0 to **192.168.12.0** and **255.255.255.240**, respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# network 192.168.12.0 255.255.255.240
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# network 238.5.5.5 255.0.0.0
238.5.5.5 / 255.0.0.0 is an invalid network
```

Common Errors

Non-unicast addresses are configured.

Related Commands

- **show ip dhcp binding**
- **show ip dhcp conflict**

1.54 next-server

Function

Run the **next-server** command to configure the boot server list that a DHCP server assigns to a DHCP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No boot server list is configured by default.

Syntax

next-server *ip-address&*<1-8>

no next-server

default next-server

Parameter Description

ip-address&<1-8>: IP address of a boot server. **<1-8>** indicates that up to eight boot server IP addresses can be entered, and the IP addresses are separated by spaces. At least one boot server needs to be configured.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

When multiple boot servers are defined, the first defined boot server has the highest priority. A DHCP client selects the next boot server only when it fails to communicate with the first defined boot server.

Examples

The following example sets the boot server for a DHCP client with an address from DHCP address pool mypool0 to **192.168.12.4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# next-server 192.168.12.4
```

Notifications

When an invalid address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# next-server 238.5.5.5
% Error: ip address(238.5.5.5) is invalid!
```

Common Errors

- Non-unicast addresses are configured.
- More than eight boot server addresses are configured.

Related Commands

N/A

1.55 option

Function

Run the **option** command to define DHCP server options.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No DHCP server option is defined by default.

Syntax

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address*&<1-16> }

no option

default option

Parameter Description

code: Code of a DHCP option.

ascii *string*: Defines an ASCII character string. The value is a case-sensitive string of 1 to 255 characters.

hex *string*: Defines a hexadecimal character string. The character length must be an even number. The value is a string of 2 to 240 characters.

ip *ip-address*&<1-16>: Defines an IP address. **<1-16>** indicates that up to 16 IP addresses can be entered, and the IP addresses are separated by spaces.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

DHCP provides a mechanism to send configuration information to hosts in a TCP/IP network. DHCP packets contain options, which are variable and can be defined as required. DHCP clients must be able to receive DHCP packets that carry option information of at least 312 bytes. The fixed data field in DHCP packets is also an option.

When this command is executed for an option multiple times in an address pool, the last configuration prevails.

The values of well-known options are fixed. Do not configure options 3, 6, 15, 44, 46, 50–55, 57–59, 61, 82, and 119.

Read the standard protocol file carefully to ensure correct configuration. For example, Option 33 is used to set static routes. This option contains one or more groups of static routes (including the destination address and gateway address). During configuration, enter an even number of IP addresses and do not set the destination IP address to **0.0.0.0**.

Examples

The following example defines Option 19 in address pool mypool0. This option determines whether a DHCP client enables IP packet forwarding. The value **0** indicates that IP packet forwarding is disabled, and the value **1** indicates that IP packet forwarding is enabled. In this example, the DHCP client enables IP packet forwarding.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# option 19 hex 01
```

The following example defines Option 33 in address pool mypool0. This option provides static route information to DHCP clients. DHCP clients obtain two static routes. For one route, the destination address is 172.16.12.0,

and the gateway address is 192.168.12.12. For the other route, the destination address is 172.16.16.0, and the gateway address is 192.168.12.16.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0
192.168.12.16
```

Notifications

When an invalid static route address is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# option 56 ip 2.2.2.2 225.5.5.5
% Error: ip address 225.5.5.5 is not valid!
```

When an invalid hexadecimal character string is configured, the following notification will be displayed:

```
Hostname(dhcp-config)# option 253 hex abcdef_
% DHCP could not parse the hexadecimal string. Check character 6 (_).
```

Common Errors

- Non-unicast addresses are configured.
- More than eight static route addresses are configured.
- An invalid hexadecimal character string is configured.

Related Commands

N/A

1.56 pool-status

Function

Run the **pool-status** command to configure whether to enable a DHCP address pool.

A created address pool is automatically enabled by default.

Syntax

pool-status { **enable** | **disable** }

Parameter Description

enable: Enables an address pool.

disable: Disables an address pool.

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

You can run this command to enable or disable an address pool temporarily when using a DHCP server.

Examples

The following example disables address pool mypool0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# pool-status disable
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.57 relay agent information

Function

Run the **relay agent information** command to enter the Option 82 matching information configuration mode from the global class configuration mode.

Run the **no** form of this command to remove this configuration.

Syntax

relay agent information

no relay agent information

Parameter Description

N/A

Command Modes

Global class configuration mode

Usage Guidelines

This command is configured on a DHCP server.

After this command is executed, the system enters the Option 82 matching information configuration mode. In this configuration mode, you can configure multiple Option 82 matching options for a class.

Examples

The following example configures a class named **myclass** and enters the Option 82 matching information configuration mode.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# relay agent information
Hostname(config-dhcp-class-relayinfo)#
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.58 relay-information hex

Function

Run the **relay-information hex** command to configure Option 82 matching information.

Run the **no** form of this command to remove this configuration.

No Option 82 matching information is configured by default.

Syntax

relay-information hex *hex-string*

no relay-information hex *hex-string*

Parameter Description

hex-string: Hexadecimal character string. The number of contained characters must be even. The value is a string of no more than 240 characters. If an asterisk (*) is added at the end of a character string, fuzzy match is used. Otherwise, exact match is used.

Command Modes

Option 82 information configuration mode under the global class configuration mode

Usage Guidelines

This command is configured on a DHCP server.

Examples

The following example configures a global class named **myclass**, which can match multiple pieces of Option 82 information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# relay agent information
Hostname(config-dhcp-class-relayinfo)# relay-information hex 0102256535
Hostname(config-dhcp-class-relayinfo)# relay-information hex 010225654565
Hostname(config-dhcp-class-relayinfo)# relay-information hex 060225654565
```

```
Hostname(config-dhcp-class-relayinfo)# relay-information hex 060223*
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.59 remark

Function

Run the **remark** command to configure identification information of a class.

Run the **no** form of this command to remove this configuration.

No identification information is configured for a class by default.

Syntax

remark *class-remark*

no remark

Parameter Description

class-remark: Identification information of a class. The value is a string of 1 to 240 characters, and spaces are allowed.

Command Modes

Global class configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

Examples

The following example sets the identification information of a global class named **myclass** to **used in #1 build**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# remark used in #1 build
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.60 service dhcp

Function

Run the **service dhcp** command to enable the DHCP Server or DHCP Relay function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCP Server and DHCP Relay functions are disabled by default.

Syntax

service dhcp

no service dhcp

default service dhcp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A DHCP server can automatically assign IP addresses and provide network configurations such as the DNS server address and default gateway address to DHCP clients.

A DHCP relay agent can forward DHCP packets between a DHCP client and a DHCP server.

The **service dhcp** command is used to enable both the DHCP Server and DHCP Relay functions. However, a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it acts as a server. Otherwise, it serves as a relay.

Examples

The following example enables the DHCP Server function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service dhcp
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.61 show ip dhcp binding

Function

Run the **show ip dhcp binding** command to display DHCP address binding information.

Syntax

show ip dhcp binding [*ip-address*]

Parameter Description

ip-address: IP address for which binding information is displayed. If this parameter is not configured, all binding information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server.

If no IP address is defined, binding information of all IP addresses is displayed. If an IP address is defined, binding information of this IP address is displayed.

Examples

The following example displays DHCP address binding information.

```
Hostname> enable
Hostname# show ip dhcp binding
Total number of clients   : 4
Expired clients          : 3
Running clients          : 1
IP address       Hardware address      Lease expiration          Type
20.1.1.1         2000.0000.2011        000 days 23 hours 59 mins   Automatic
```

Table 1-3 Output Fields of the show ip dhcp binding Command

Field	Description
IP address	IP address assigned to a DHCP client
Hardware address	Hardware address of a DHCP client

Field	Description
Lease expiration	Lease expiration time ● **Infinite**: There is no time limitation. ● **IDLE**: The current address is idle because the lease of the address is not renewed or a DHCP client releases the IP address actively.
Type	Address binding type ● **Automatic**: IP addresses are automatically assigned. ● **Manual**: IP addresses are manually assigned.

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.62 show ip dhcp conflict

Function

Run the **show ip dhcp conflict** command to display IP address conflict records of a DHCP server.

Syntax

show ip dhcp conflict

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays address conflict records of a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp conflict
```

```
IP address    Detection Method
192.168.12.1          Ping
```

Table 1-4 Output Fields of the show ip dhcp conflict Command

Field	Description
IP address	IP address that cannot be assigned to a DHCP client
Detection Method	Conflict detection method

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.63 show ip dhcp database

Function

Run the **show ip dhcp database** command to display the running status of the database backup function of a DHCP server.

Syntax

show ip dhcp database

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the running status of the database backup function of a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp database
Enable        :No
```

```
Status         :ready
Save File      :Default
Successs       :0
Failures       :0
Interval Time   :86400
```

Table 1-5 Output Fields of the show ip dhcp database Command

Field	Description
Enable	Indicates whether the database backup function is enabled.
Status	Data restoration status.
Save File	Path of Data saving file.
Success	Number of successful data savings.
Failures	Number of failed data savings.
Interval Time	Data saving interval.

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.64 show ip dhcp dns dynamic

Function

Run the **show ip dhcp dns dynamic** command to display the DNS server address obtained from an external DHCP server when the device works in PPPoE or DHCP client mode.

Syntax

show ip dhcp dns dynamic

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays lease information about an assigned IP address, that is, the DNS server address obtained from an external DHCP server when the device works in PPPoE or DHCP client mode.

```
Hostname> enable
Hostname# show ip dhcp dns dynamic
Get dynamic dns is open
No.  DYNAMIC-DNS
-  -----
1    20.1.1.12
```

Table 1-6 Output Fields of the show ip dhcp dns dynamic Command

Field	Description
Get dynamic dns is	• **open**: The function of obtaining a DNS server address from an external DHCP server is enabled. • **close**: The function of obtaining a DNS server address from an external DHCP server is disabled.
DYNAMIC-DNS	DNS server address obtained from an external DHCP server when the device works in PPPoE or DHCP client mode.

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.65 show ip dhcp history

Function

Run the **show ip dhcp history** command to display historical lease records.

Syntax

show ip dhcp history

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays historical lease records.

```
Hostname> enable
Hostname# show ip dhcp history
Expired clients         : 3
IP address       Hardware address      Lease expiration          Vlan/Relay
10.1.1.5         2222.abcd.47ac        IDLE                      4097
10.1.1.4         2222.abcd.47ae        IDLE                      4097
10.1.1.3         2222.abcd.47ad        IDLE                      4097
Running clients         : 0
```

Table 1-7 Output Fields of the show ip dhcp history Command

Field	Description
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Lease expiration time ● **Infinite**: There is no time limitation. ● **IDLE**: The current address is idle because the lease of the address is not renewed or a DHCP client releases the IP address actively.
Vlan/Relay	If a DHCP client applies for an IP address through a DHCP relay agent, the DHCP relay agent address is displayed. Otherwise, the index of the port that receives DHCP packets is displayed.
Running clients	Total number of online clients

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.66 show ip dhcp identifier

Function

Run the **show ip dhcp identifier** command to display the address pool ID and address usage of a DHCP server.

Syntax

show ip dhcp identifier

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The address pool ID can be used to construct an object identifier (OID) of a Management Information Base (MIB) to access specific content of an address pool.

Examples

The following example displays the address pool ID and address usage of a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp identifier
Pool  name    Identifier     Total    Distributed  Remained
----  -----  -----  -----  ----
wwp          597455782    65533       0           65533
```

Table 1-8 Output Fields of the show ip dhcp identifier Command

Field	Description
Pool name	Address pool name
Identifier	Address pool ID
Total	Total number of assignable addresses in an address pool
Distributed	Number of assigned addresses
Remained	Number of unassigned and reusable addresses

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.67 show ip dhcp pool

Function

Run the **show ip dhcp pool** command to display the address pool status and utilization of a DHCP server.

Syntax

show ip dhcp pool [*pool-name*]

Parameter Description

pool-name: Name of an address pool whose information is to be displayed. If this parameter is not configured, configurations of all address pools are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the address pool status and utilization of a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp pool
Pool  name      Total    Distributed  Remained   Percentage
----  -----  -----  ----   -----
net20        253         11          242       4.34782
test         0           0           0         0.00000
```

Table 1-9 Output Fields of the show ip dhcp pool Command

Field	Description
Pool address	Address pool name
Total	Total number of assignable addresses in an address pool
Distributed	Number of assigned addresses

Field	Description
Remained	Number of unassigned and reusable addresses
Percentage	Address utilization of an address pool

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.68 show ip dhcp relay-statistics

Function

Run the **show ip dhcp relay-statistics** command to display statistics of a DHCP relay agent.

Syntax

show ip dhcp relay-statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics of a DHCP relay agent.

```
Hostname> enable
Hostname# show ip dhcp relay-statistics
Cycle mode              0
Message                Count
Discover                0
Offer                  0
Request                 0
Ack                    0
```

```
Nak                  0
Decline               0
Release               0
Info                 0
Bad                  0
Direction             Count
Rx client             0
Rx client uni          0
Rx client bro          0
Tx client             0
Tx client uni          0
Tx client bro          0
Rx server             0
```

Table 1-10 Output Fields of the show ip dhcp relay-statistics Command

Field	Description
Cycle mode	• **0**: Packets can be sent to multiple DHCP servers. • **1**: Packets can be sent only to the specified DHCP server.
Discover	Total number of DISCOVER packets received
Offer	Total number of OFFER packets received
Request	Total number of REQUEST packets received
Ack	Total number of ACK packets received
Nak	Total number of NAK packets received
Decline	Total number of DECLINE packets received
Release	Total number of RELEASE packets received
Info	Total number of INFORM packets received
Bad	Total number of abnormal DHCP packets received
Direction	Packet statistics by direction
Rx client	Total number of packets received from clients
Rx client uni	Total number of unicast packets received from clients
Rx client bro	Total number of broadcast packets received from clients
Tx client	Total number of packets forwarded to clients
Tx client uni	Total number of unicast packets forwarded to clients
Tx client bro	Total number of broadcast packets forwarded to clients
Rx server	Total number of packets received from a server

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.69 show ip dhcp server detect

Function

Run the **show ip dhcp server detect** command to display the list of detected rogue servers.

Syntax

show ip dhcp server detect

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the list of rogue servers detected by a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp server detect
The DHCP Server information(total: 1):
NO.   SERVER IP      INTERFACE
1     10.1.10.40    GigabitEthernet 0/1
```

Table 1-11 Output Fields of the show ip dhcp server detect Command

Field	Description
The DHCP Server information(total: x)	Rogue servers detected by a DHCP server, *x* in total
NO.	No.
SERVER IP	IP address of a rogue server
INTERFACE	Interface over which a rogue server is detected

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.70 show ip dhcp server statistics

Function

Run the **show ip dhcp server statistics** command to display statistics of a DHCP server.

Syntax

show ip dhcp server statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics of a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp server statistics
Address pools           2
Lease counter           4
Active Lease Counter    0
Expired Lease Counter    4
Malformed messages       0
Dropped messages         0

Message                Received
BOOTREQUEST          216
DHCPDISCOVER         33
DHCPREQUEST          25
```

```
DHCPDECLINE           0
DHCPRELEASE           1
DHCPINFORM            150

Message                 Sent
BOOTREPLY             16
DHCPOFFER             9
DHCPACK                7
DHCPNAK                0
----------------
recv                     0
send                    0
```

Table 1-12 Output Fields of the show ip dhcp server statistics Command

Field	Description
Address pools	Number of address pools
Lease counter	Number of assigned leases
Active Lease Counter	Number of online leases
Expired Lease Counter	Number of aged leases
Automatic bindings	Number of automatically bound IP addresses
Manual bindings	Number of manually bound IP addresses
Expired bindings	Number of expired bindings
Malformed messages	Number of abnormal DHCP packets received
Dropped messages	Number of discarded packets
Message Received	Number of each type of DHCP packets received
Message Sent	Number of each type of DHCP packets sent
BOOTREQUEST	Total number of BOOTP request packets
DHCPDISCOVER	Total number of DISCOVER packets received
DHCPREQUEST	Total number of REQUEST packets
DHCPDECLINE	Total number of DECLINE packets
DHCPRELEASE	Total number of RELEASE packets
DHCPINFORM	Total number of INFORM packets
BOOTREPLY	Total number of BOOTP reply packets
DHCPOFFER	Total number of OFFER packets
DHCPACK	Total number of ACK packets

Field	Description
DHCPNAK	Total number of NAK packets
recv	Total number of received packets
send	Total number of sent packets

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1.71 show ip dhcp socket

Function

Run the **show ip dhcp socket** command to display the socket index used by a DHCP server.

Syntax

show ip dhcp socket

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the socket index used by a DHCP server.

```
Hostname> enable
Hostname# show ip dhcp socket
dhcp socket = 47.
```

Table 1-13 Output Fields of the show ip dhcp socket Command

Field	Description

Field	Description
dhcp socket	Socket index

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.72 update arp

Function

Run the **update arp** command to enable a DHCP server to add trusted ARP entries during address assignment.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No trusted ARP entry is added during DHCP address assignment by default.

Syntax

update arp

no update arp

default update arp

Parameter Description

N/A

Command Modes

DHCP address pool configuration mode

Default Level

14

Usage Guidelines

This command is configured on a DHCP server. After this command is configured for an address pool, the DHCP server adds trusted ARP entries when assigning IP addresses from the address pool. A trusted ARP entry has a higher priority than a dynamic ARP entry and is not overridden by a dynamic ARP entry.

Examples

The following example enables a DHCP server to add trusted ARP entries when assigning addresses from address pool mypool0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# update arp
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1 DHCP Client Commands

Command	Function
ip address dhcp	Enable an Ethernet, Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), or frame relay (FR) interface to obtain IP addresses through Host Configuration Protocol (DHCP).
show dhcp lease	Display lease information of a DHCP client.

1.1 ip address dhcp

Function

Run the **ip address dhcp** command to enable an Ethernet, Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), or frame relay (FR) interface to obtain IP addresses through Host Configuration Protocol (DHCP).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface can obtain an IP address through DHCP by default.

Syntax

ip address dhcp

no ip address dhcp

default ip address dhcp

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When a DHCP client requests an IP address from a DHCP server, it also requires the DHCP server to provide the following configuration parameters:

- **DHCP Option 1**: Subnet mask of the client
- **DHCP Option 3**: Gateway in the same subnet
- **DHCP Option 6**: Domain name server (DNS) information
- **DHCP Option 15**: Host domain name
- **DHCP Option 44**: Windows Internet Name Service (WINS) server information

Examples

The following example enables GigabitEthernet 0/1 to obtain an IP address automatically.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1) ip address dhcp
```

Notifications

N/A

Common Errors

The DHCP Client function is enabled on an L2 interface.

Related Commands

N/A

1.2 show dhcp lease

Function

Run the **show dhcp lease** command to display lease information of a DHCP client.

Syntax

show dhcp lease

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays lease information of a DHCP client.

```
Hostname> enable
Hostname# show dhcp lease
Temp IP addr: 192.168.5.71  for peer on Interface: FastEthernet0/0
Temp  sub net mask: 255.255.255.0
DHCP Lease server: 192.168.5.70, state: 7 Bound
DHCP transaction id: 337beed
Lease: 600 secs,  Renewal: 300 secs,  Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
Next timer fires after: 00:04:29
Retry count: 0   Client-ID: 0100d0f82233e34769676162697445746865726E6574302F31
```

Table 1-1 Output Fields of the show dhcp lease Command

Field	Description
Temp IP addr	IP address assigned to a DHCP client
for peer on Interface	Interface over which an IP address is applied for

Field	Description
Temp sub net mask	Subnet mask of an interface address
DHCP Lease serve	Server IP address
state	Lease status
DHCP transaction id	Packet transaction ID
Lease	Lease time
Renewal	Lease renewal time
Rebind	IP address rebinding time
Temp default-gateway addr	Gateway address
Next timer fires after	Next time for triggering the timer

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1 DHCP Snooping Commands

Command	Function
clear ip dhcp snooping binding	Clear all dynamic users in the Dynamic Host Configuration Protocol (DHCP) snooping binding database.
ip dhcp snooping	Enable DHCP Snooping globally.
ip dhcp snooping bootp-bind	Enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.
ip dhcp snooping check-giaddr	Enable DHCP Snooping to support relay request packet processing.
ip dhcp snooping database write-delay	Write all dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time.
ip dhcp snooping database write-to-flash	Write dynamic user information in the DHCP Snooping binding database to flash in real time.
ip dhcp snooping information option	Add Option 82 to DHCP request packets.
ip dhcp snooping information option format remote-id	Set the Remote ID sub-option to a user-defined string or the host name when Option 82 is in extended mode.
ip dhcp snooping monitor	Enable DHCP Snooping monitoring globally.
ip dhcp snooping station-move aging	Enable DHCP Snooping to fast age terminal migration entries.
ip dhcp snooping station-move permit	Enable DHCP Snooping to support binding entry migration.
ip dhcp snooping suppression	Configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.
ip dhcp snooping trust	Configure an interface as a DHCP Snooping trusted port.
ip dhcp snooping verify mac-address	Enable source MAC address verification.
ip dhcp snooping vlan	Enable DHCP Snooping on a specified VLAN.
ip dhcp snooping vlan information option change-vlan-to vlan	Set the VLAN filed in Circuit ID of Option 82 in extended mode to a specified VLAN.

ip dhcp snooping vlan information option format-type circuit-id string	Set Circuit ID to user-defined content for forwarding when Option 82 is in extended mode.
ip dhcp snooping vlan max-user	Configure the maximum number of users bound to a VLAN.
renew ip dhcp snooping database	Import information in the current backup file to the DHCP Snooping binding database.
show ip dhcp snooping	Display the DHCP Snooping configurations.
show ip dhcp snooping binding	Display user information in the DHCP Snooping binding database.

1.1 clear ip dhcp snooping binding

Function

Run the **clear ip dhcp snooping binding** command to clear all dynamic users in the Dynamic Host Configuration Protocol (DHCP) snooping binding database.

Syntax

clear ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ip-address: IP address of a user.

mac-address: Media Access Control (MAC) address of a user.

vlan-id: Virtual local area network (VLAN) ID of a user.

interface-type interface-number: Interface of a user.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After this command is run, all DHCP users who access the interface with IP Source Guard enabled need to re-apply for IP addresses. Otherwise, they cannot access the Internet.

Examples

The following example clears all dynamic users in the DHCP Snooping binding database.

```
Hostname> enable
Hostname# clear ip dhcp snooping binding
```

Notifications

N/A

Platform Description

N/A

1.2 ip dhcp snooping

Function

Run the **ip dhcp snooping** command to enable DHCP Snooping globally.

Run the **no** form of this command to disable this function.

DHCP Snooping is disabled globally by default.

Syntax

ip dhcp snooping

no ip dhcp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After DHCP Snooping is enabled globally, you can run the **show ip dhcp snooping** command to check whether this function is enabled.

Examples

The following example enables DHCP Snooping globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping
```

Notifications

When this command is run to enable DHCP Snooping after DHCP Snooping monitoring is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Conflict with DHCP snooping monitor".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip dhcp snooping bootp-bind

Function

Run the **ip dhcp snooping bootp-bind** command to enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.

Run the **no** form of this command to disable this function.

DHCP Snooping does not support BOOTP binding by default.

Syntax

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After being enabled, DHCP Snooping snoops and forwards only BOOTP packets by default. After a BOOTP client successfully applies for an IP address, DHCP Snooping adds the BOOTP user to the static binding database.

Examples

The following example enables DHCP Snooping to support BOOTP binding.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping bootp-bind
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip dhcp snooping check-giaddr

Function

Run the **ip dhcp snooping check-giaddr** command to enable DHCP Snooping to support relay request packet processing.

Run the **no** form of this command to disable this function.

DHCP Snooping does not support relay request packet processing by default.

Syntax

ip dhcp snooping check-giaddr

no ip dhcp snooping check-giaddr

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this function is enabled, services (IP Source Guard and Dot1x authentication) using DHCP Snooping binding entries generated based on relay requests cannot be deployed. Otherwise, users fail to access the Internet.

After this function is enabled, the **ip dhcp snooping verify mac-address** command cannot be configured. Otherwise, DHCP relay request packets are discarded, and users fail to obtain addresses.

Examples

The following example enables DHCP Snooping to support relay request packet processing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping check-giaddr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip dhcp snooping database write-delay

Function

Run the **ip dhcp snooping database write-delay** command to write all dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time.

Run the **no** form of this command to disable this function.

The function of writing all dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time is not configured by default.

Syntax

ip dhcp snooping database write-delay *time*

no ip dhcp snooping database write-delay

Parameter Description

time: Period for saving database records, in seconds. The value range is from 600 to 86400.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to write dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time. This prevents user information loss after the device restarts, and there is no need to re-obtain IP addresses to restore communication.

Note

A high saving frequency reduces the lifespan of the flash.

Examples

The following example writes all dynamic user information in the DHCP Snooping binding database to a flash memory every 3600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-delay 3600
```

Notifications

N/A

Common Errors

The configured period exceeds the limit.

Platform Description

N/A

Related Commands

N/A

1.6 ip dhcp snooping database write-to-flash

Function

Run the **ip dhcp snooping database write-to-flash** command to write dynamic user information in the DHCP Snooping binding database to flash in real time.

Syntax

ip dhcp snooping database write-to-flash

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Wireless user information is not written to flash.

If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored because the two versions correspond to different flashes.

Examples

The following example writes dynamic user information in the DHCP Snooping binding database to flash in real time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-to-flash
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip dhcp snooping information option

Function

Run the **ip dhcp snooping information option** command to add Option 82 to DHCP request packets.

Run the **no** form of this command to remove this configuration.

Option 82 is not added to DHCP request packets by default.

Syntax

ip dhcp snooping information option [**standard-format** | **user-defined**]

no ip dhcp snooping information option [**standard-format** | **user-defined**]

Parameter Description

standard-format: Uses the standard format for Option 82.

user-defined: Uses the user-defined format for Option 82.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to add Option 82 to DHCP request packets so that a DHCP server assigns addresses based on Option 82.

When enabled, Option 82 is in extended mode by default.

Caution

Option 82 for DHCP Snooping is exclusive to that for DHCP Relay.

Examples

The following example adds Option 82 to DHCP request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option
```

Notifications

N/A

Common Errors

Option 82 for DHCP Snooping and that for DHCP Relay are enabled at the same time. As a result, Option 82 in the DHCP packets is incorrect.

Platform Description

N/A

Related Commands

N/A

1.8 ip dhcp snooping information option format remote-id

Function

Run the **ip dhcp snooping information option format remote-id** command to set the **Remote ID** sub-option to a user-defined string or the host name when Option 82 is in extended mode.

Run the **no** form of this command to remove this configuration.

Remote ID in Option 82 is not set to a user-defined string or host name by default.

Syntax

ip dhcp snooping information option format remote-id { **string** *ascii-string* | **hostname** }

no ip dhcp snooping information option format remote-id

Parameter Description

string *ascii-string*: Sets **Remote ID** in Option 82 to a user-defined string.

hostname: Sets **Remote ID** in Option 82 to the host name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in extended mode, this command is used to customize the content of **Remote ID** in Option 82.

Examples

The following example sets **Remote ID** in Option 82 to the host name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option format remote-id hostname
```

Notifications

When the value of the *ascii-string* parameter exceeds 63 characters, the following notification will be displayed:

```
% Failed to execute command, because of "Remote-ID string cannot exceed 63 characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip dhcp snooping monitor

Function

Run the **ip dhcp snooping monitor** command to enable DHCP Snooping monitoring globally.

Run the **no** form of this command to disable this function.

DHCP Snooping monitoring is disabled globally by default.

Syntax

ip dhcp snooping monitor

no ip dhcp snooping monitor

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the DHCP Snooping monitoring function is enabled, DHCP Snooping only copies DHCP packets and generates binding entries based on the interaction status, but does not check the validity of the packets.

The DHCP Snooping monitoring and DHCP Snooping functions are mutually exclusive.

After the DHCP Snooping monitoring function is enabled, if the VLAN field in the **show ip dhcp snooping binding** command is set to **0**, VLAN information is not carried in binding entries generated for routed ports.

Examples

The following example enables DHCP Snooping monitoring globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping monitor
```

Notifications

When DHCP Snooping monitoring is configured after DHCP Snooping is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Conflict with DHCP snooping".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip dhcp snooping station-move aging

Function

Run the **ip dhcp snooping station-move aging** command to enable DHCP Snooping to fast age terminal migration entries.

Run the **no** form of this command to disable this function.

Fast aging of client migration entries is enabled for DHCP Snooping by default.

Syntax

ip dhcp snooping station-move aging

no ip dhcp snooping station-move aging

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a terminal is migrated between different sub VLANs of the same super VLAN and a binding entry is generated in the new sub VLAN, this command is used to enable DHCP Snooping to fast age binding entries in other sub VLANs.

Examples

The following example disables fast aging of terminal migration entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dhcp snooping station-move aging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ip dhcp snooping station-move permit

Function

Run the **ip dhcp snooping station-move permit** command to enable DHCP Snooping to support binding entry migration.

Run the **no** form of this command to disable this function.

DHCP Snooping does not support binding entry migration by default.

Syntax

ip dhcp snooping station-move permit

no ip dhcp snooping station-move permit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When no DHCP request for an IP address is initiated after terminal migration, this command is used to enable DHCP Snooping to find the latest binding entries in the super VLAN based on the target sub VLAN and generates binding entries of the target sub VLAN.

Examples

The following example enables DHCP Snooping to support binding entry migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping station-move permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip dhcp snooping suppression

Function

Run the **ip dhcp snooping suppression** command to configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.

Run the **no** form of this command to remove this configuration.

No interface is configured in the suppression state by default.

Syntax

ip dhcp snooping suppression

no ip dhcp snooping suppression

Parameter Description

N/A

Command Modes

Interface configuration mode

Wireless security configuration mode

Default Level

14

Usage Guidelines

This command is used to reject all DHCP packets on an untrusted port, that is, to forbid all users on this port to apply for addresses via DHCP.

This command can be configured only on L2 switching ports or aggregation ports (APs).

Examples

The following example configures GigabitEthernet 0/1 in the suppression state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping suppression
```

Notifications

When this command is configured on a DHCP trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port, AP, or L2 encapsulation sub-interface for wired access, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ip dhcp snooping trust

Function

Run the **ip dhcp snooping trust** command to configure an interface as a DHCP Snooping trusted port.

Run the **no** form of this command to remove this configuration.

All interfaces are DHCP Snooping untrusted ports by default.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure interfaces connected to legitimate DHCP servers as trusted ports. DHCP response packets received on trusted ports are forwarded normally, while those received on untrusted ports are discarded.

This command can be configured only on L2 switching ports, APs, or encapsulation sub-interfaces.

Caution

Generally, uplink interfaces, that is, interfaces connected to trusted DHCP servers are configured as trusted ports.

Examples

The following example configures GigabitEthernet 0/1 as a DHCP Snooping trusted port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping trust
```

Notifications

When an interface configured with other access security control options is configured as a DHCPv6 Snooping trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port, AP, or L2 encapsulation sub-interface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ip dhcp snooping verify mac-address

Function

Run the **ip dhcp snooping verify mac-address** command to enable source MAC address verification.

Run the **no** form of this command to disable this function.

Source MAC address verification is disabled by default.

Syntax

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After source MAC address verification is enabled, the MAC addresses in link layer headers and the **CLIENT MAC** fields in DHCP request packets from untrusted ports are checked for consistence. If the verification fails, packets are discarded.

Examples

The following example enables source MAC address verification.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping verify mac-address
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ip dhcp snooping vlan

Function

Run the **ip dhcp snooping vlan** command to enable DHCP Snooping on a specified VLAN.

Run the **no** form of this command to disable this function.

After DHCP Snooping is enabled globally, it takes effect to all VLANs by default.

Syntax

ip dhcp snooping vlan { *vlan-range* | { *vlan-min* [*vlan-max*] } }

no ip dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

Parameter Description

vlan-range: Range of VLANs to which DHCP Snooping takes effect. The value is a character string, for example 1, 3–5, 7, and 9–11.

vlan-min: Minimum ID of a VLAN to which DHCP Snooping takes effect. The value range is from 1 to 4094.

vlan-max: Maximum ID of a VLAN to which DHCP Snooping takes effect. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable or disable DHCP Snooping for a specified VLAN. This function takes effect only when DHCP Snooping is enabled globally.

Examples

The following example enables DHCP Snooping for VLAN 1000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping vlan 1000
```

The following example enables DHCP Snooping for VLAN 1 to VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping vlan 1-10
```

Notifications

When the configured VLAN ID is beyond the range of 1 to 4094, the following notification will be displayed:

```
% Failed to execute command, because of "Not supported vlan range".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ip dhcp snooping vlan information option change-vlan-to vlan

Function

Run the **ip dhcp snooping vlan information option change-vlan-to vlan** command to set the VLAN filed in **Circuit ID** of Option 82 in extended mode to a specified VLAN.

Run the **no** form of this command to remove this configuration.

When Option 82 is in extended mode, the VLAN in **Circuit ID** is not configured as the specified VLAN by default.

Syntax

ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

no ip dhcp snooping vlan *vlan-id* **information option**

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in extended mode, this command is used to change the value of the VLAN field in **the Circuit ID** of Option 82 to a specified VLAN.

Examples

The following example changes VLAN 4094 in **Circuit ID** of Option 82 to VLAN 4093 when Option 82 is added to DHCP request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip dhcp snooping vlan information option format-type circuit-id string

Function

Run the **ip dhcp snooping vlan information option format-type circuit-id string** command to set **Circuit ID** to user-defined content for forwarding when Option 82 is in extended mode.

Run the **no** form of this command to remove this configuration.

When Option 82 is in extended mode, **Circuit ID** is not set to user-defined content for forwarding by default.

Syntax

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

no ip dhcp snooping vlan *vlan-id* **information option**

Parameter Description

vlan-id: ID of the VLAN where DHCP request packets are from.

ascii-string: User-defined **Circuit ID** content. The value is a string of 3 to 63 bytes in ASCII format.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in extended mode, this command is used to customize **Circuit ID** in Option 82.

Examples

The following example sets **Circuit ID** of Option 82 to port-name when Option 82 is added to DHCP request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option
format-type circuit-id string port-name
```

Notifications

When the user-defined character string is not 3 to 63 characters, the following notification is displayed:

```
% Failed to execute command, because of "Circuit-ID string must be 3 to 63 characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip dhcp snooping vlan max-user

Function

Run the **ip dhcp snooping vlan max-user** command to configure the maximum number of users bound to a VLAN.

Run the **no** form of this command to remove this configuration.

The maximum number of users bound to a VLAN is not configured by default.

Syntax

ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

no ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

Parameter Description

vlan-range: Range of VLANs to which DHCP Snooping takes effect.

user-number: Maximum number of allowed users. The value range is from 1 to 26624.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of users bound based on the interface and VLAN, so as to prevent forge DHCP packets in accordance with the network topology.

Examples

The following example binds a maximum of 30 users to VLANs 1 to 10 and VLAN 20 on interface 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user 30
```

Notifications

When an interface from a specified VLAN is a DHCP Snooping trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in interface
GigabitEthernet 0/1".
```

When the number of users bound to a VLAN on a specified interface exceeds the maximum number of allowed users configured in the command, the following notification will be displayed:

```
% Failed to execute command, because of "New max address number little more than the
current".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 renew ip dhcp snooping database

Function

Run the **renew ip dhcp snooping database** command to import information in the current backup file to the DHCP Snooping binding database.

Syntax

renew ip dhcp snooping database

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to import information in the current backup file to the DHCP Snooping binding database.

Note

- Lease expiration records in the backup file are ignored.
- Only records that do not exist in the database are added.

Examples

The following example imports information in the current backup file to the DHCP Snooping binding database.

```
Hostname> enable
Hostname# renew ip dhcp snooping database
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ip dhcp snooping

Function

Run the **show ip dhcp snooping** command to display the DHCP Snooping configurations.

Syntax

show ip dhcp snooping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays DHCP Snooping configurations.

```
Hostname> enable
Hostname# show ip dhcp snooping
Switch DHCP snooping status                 :   ENABLE
DHCP snooping verify hardware address status    :   DISABLE
DHCP snooping database write-delay time       :   0 seconds
DHCP snooping option 82 status               :   DISABLE
DHCP snooping Support bootp bind status       :   DISABLE
Interface                                    Trusted          Rate limit(pps)
GigabitEthernet 0/1                            YES             unlimited
Default                                      No
```

Table 1-1 Output Fields of the show ip dhcp snooping Command

Field	Description
Switch DHCP snooping status	Indicates whether DHCP Snooping is enabled globally.
DHCP snooping verify hardware address status	Status of the switch for verifying the source MAC address in DHCP Snooping packets.
DHCP snooping database write-delay time	Interval for writing data to a backup file.
DHCP snooping option 82 status	Indicates whether Option 82 is added to DHCP request packets.

DHCP snooping Support Bootp bind status	Indicates whether to enable DHCP Snooping to support BOOTP binding.
Interface	Interface name.
Trusted	Indicates whether an interface is a trusted port.
Rate limit	Rate limit for DHCP packets on an interface.

Notifications

N/A

Platform Description

N/A

1.21 show ip dhcp snooping binding

Function

Run the **show ip dhcp snooping binding** command to display user information in the DHCP Snooping binding database.

Syntax

show ip dhcp snooping binding

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays user information in the DHCP Snooping binding database.

```
Hostname> enable
Hostname# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS        IPADDRESS      LEASE(SEC)   TYPE         VLAN  INTERFACE
1     0000.0000.0001    1.1.1.1        78128       DHCP-Snooping 1
GigabitEthernet 0/1
```

Table 1-2 Output Fields of the show ip dhcp snooping binding Command

Field	Description
Total number of bindings	Current number of bindings in the DHCP Snooping binding database.
No.	Record number.
MACADDRESS	MAC address of a user.
IPADDRESS	IP address of a user.
LEASE (SEC)	Lease time of a record.
TYPE	Record type.
VLAN	VLAN of a user.
INNER-VLAN	ID of the inner VLAN of a user. This field is applicable to products that support QinQ VLAN tag termination.
INTERFACE	Interface to which a user's terminal connects.

Notifications

N/A

Platform Description

N/A

1 DNS Commands

Command	Function
clear host	Clear the dynamic domain name cache entries.
clear dns proxy host	Clear the dynamic domain name cache entries on the DNS proxy.
ip domain-lookup	Enable DNS for domain name resolution, or enable DNS for domain name resolution and specify the source interface and IP address for domain name resolution.
ip host	Configure a static mapping between a host name and an IP address.
ip name-server	Configure an IPv4/IPv6 address for a DNS server.
ipv6 host	Configure a static mapping between a host name and an IPv6 address.
ip dns proxy cache	Enable the function of caching dynamic entries on the DNS proxy.
ip dns proxy enable	Enable the DNS proxy function.
ip dns proxy host	Configure a static mapping between a host name and an IP address on the DNS proxy.
ip dns proxy nameserver	Configure the IP address of a DNS server on the DNS proxy.
ip dns proxy port-range	Configure the range of a port used for query in upper-level DNS servers.
ip dns proxy ttl	Configure the time to live (TTL) of the reply packet in response to a static entry.
show hosts	Display the DNS configuration.
show dns proxy hosts	Display the entries on the DNS proxy.
show dns proxy statistics	Display the DNS proxy packet statistics.

1.1 clear host

Function

Run the **clear host** command to clear the dynamic domain name cache entries.

Syntax

clear host [* | *host-name*]

Parameter Description

host-name: Name of a host whose dynamic domain name entries need to be deleted.

*****: Deletes all dynamic domain name entries.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Mapping records in the domain name cache are sourced from the following:

- Static configuration by running the **ip host** or **ipv6 host** command;
- Dynamic learning through DNS.

This command can be used to delete domain name records dynamically learned through DNS.

Examples

The following example clears all the dynamic domain name cache entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#clear host *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear dns proxy host

Function

Run the **clear dns proxy host** command to clear the dynamic domain name cache entries on the DNS proxy.

Syntax

clear dns proxy host [* | *host-name*]

Parameter Description

host-name: Name of a host whose dynamic domain name cache entries need to be deleted.

*****: Deletes all dynamic domain name entries.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Mapping records in the domain name cache are sourced from the following:

- Static configuration by running the **ip dns proxy host** command;
- Dynamic learning through DNS.

This command can be used to delete domain name records dynamically learned through DNS.

Examples

The following example deletes all the dynamic domain name cache entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# clear dns proxy host *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip domain-lookup

Function

Run the **ip domain-lookup** command to enable DNS for domain name resolution, or enable DNS for domain name resolution and specify the source interface and IP address for domain name resolution.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DNS domain name resolution function is enabled and the function of domain name resolution using a specified source interface or IP address is disabled by default.

Syntax

ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] [**source** { *interface-type interface-number* | **ip** *ipv4-address* | **ipv6** *ipv6-address* }]]

no ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] **source**]

default ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] **source**]

Parameter Description

oob: Configures out-of-band management.

via *mgmt-name*: Specifies the outbound management interface of packets.

vrf *vrf-name*: Specifies a VRF instance. If this parameter is not specified, it indicates the public network instance.

source: Specifies the source interface or source IP address for domain name resolution.

interface-type interface-number: L3 interface type and interface number.

ip *ipv4-address*: IPv4 address.

ipv6 *ipv6-address*: IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, no source interface is specified, and the source IP address of a DNS query packet is decided through the routing process.

If a source interface is specified in the command, when an IPv4 DNS query packet is sent, the primary IPv4 address of the source interface is used as the source address of the DNS query packet. When an IPv6 DNS query packet is sent, the first effective IPv6 address of the source interface is used as the source address of the DNS query packet. If no address is configured for a source interface, a DNS query packet fails to be sent.

If an IPv4 source address is specified in the command, when an IPv4 DNS query packet is sent, the configured IPv4 address serves as the source address of the IPv4 DNS query packet, and the sending of an IPv6 DNS query packet will fail. If an IPv6 source address is specified in the command, when an IPv6 DNS query packet is sent, the configured IPv6 address serves as the source address of the IPv6 DNS query packet, and the sending of an IPv4 DNS query packet will fail.

Caution

An effective IPv6 address is a unicast address and it cannot be either a local link address or a loopback address.

Examples

The following example disables the DNS domain name resolution and disables the function of domain name resolution using a specified source interface or IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip domain-lookup
```

Notifications

When the configured interface is not an L3 interface, the following notification will be displayed:

```
% Error: AggregatePort 1 is not l3 layer!
```

When the configured address is an illegitimate IPv4 address, for example, a loopback address, the following notification will be displayed:

```
% Invalid ip(1.1.1.1) address!
```

When the configured address is an illegitimate IPv6 address, for example, a local-link address or a loopback address, the following notification will be displayed:

```
% Invalid ipv6(0000::1) address!
```

Common Errors

- The configured source interface for DNS domain name resolution is an L2 interface and this command cannot be successfully configured.
- The configured source IP address for DNS domain name resolution is not a unicast address and this command cannot be successfully configured.

Platform Description

N/A

Related Commands

N/A

1.4 ip host

Function

Run the **ip host** command to configure a static mapping between a host name and an IP address.

Run the **no** form of this command to remove this configuration.

No static mapping between a host name and an IP address is configured by default.

Syntax

ip host [**oob**] *host-name* [*telnet-port*] *ip-address* [**via** *mgmt-name*]

ip host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ip-address*

no ip host [**oob**] *host-name* [*telnet-port*] *ip-address* [**via** *mgmt-name*]

no ip host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ip-address*

Parameter Description

oob: Configures out-of-band management.

vrf *vrf-name*: Configures a VRF instance.

host-name: Host name of a device.

telnet-port: Telnet port of a device. The value range is from 0 to 65535. The default value is 0.

ip-address: IP address of a device.

via *mgmt-name*: Specifies the outbound management interface of packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the static mapping between host name www.test.com and IP address 192.168.5.243.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip host www.test.com 192.168.5.243
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show hosts**
- **clear host**

1.5 ip name-server

Function

Run the **ip name-server** command to configure an IPv4/IPv6 address for a DNS server.

Run the **no** form of this command to remove this configuration.

No DNS server is configured by default.

Syntax

ip name-server [**oob**] { *ipv4-address*&<1-6> | *ipv6-address*&<1-6> } [**via** *mgmt-name*]

ip name-server [**vrf** *vrf-name*] { *ipv4-address*&<1-6> | *ipv6-address*&<1-6> }

no ip name-server [**oob**] { *ipv4-address* | *ipv6-address* } [**via** *mgmt-name*]

no ip name**-**server **[** vrf ***vrf-name*** **] { *ipv4-address* | *ipv6-address* } [** via ***mgmt-name* **]Parameter Description**

oob: Configures out-of-band management.

ipv4-address&<1-6>: IPv4 address of a DNS server. &<1-6> indicates that the IPv4 addresses of up to six DNS servers can be configured.

ipv6-address&<1-6>: IPv6 address of a DNS server. &<1-6> indicates that the IPv6 addresses of up to six DNS servers can be configured.

vrf *vrf-name*: Specifies a VRF instance.

via *mgmt-name*: Specifies the outbound management interface of packets when the **oob** parameter is set.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Dynamic domain name resolution can be performed only after a DNS server is configured.

This command is used to configure the IPv4/IPv6 addresses for DNS servers. Each time this command is run, the device will add one DNS server. When a domain name cannot be obtained from the first server, the device tries to send a DNS request to subsequent servers until it receives a correct reply.

The system supports up to six DNS servers. If the *ipv4-address* or *ipv6-address* parameter is specified when you delete a DNS server, only the specified server will be deleted. Otherwise, the IP addresses of all DNS servers will be deleted.

Examples

The following example sets the IPv4 address of a DNS server to 192.168.5.134 and the management interface to 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip name-server 192.168.5.134 via mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ipv6 host

Function

Run the **ipv6 host** command to configure a static mapping between a host name and an IPv6 address.

Run the **no** form of this command to remove this configuration.

No static mapping between a host name and an IPv6 address is configured by default.

Syntax

ipv6 host [**oob**] *host-name* [*telnet-port*] *ipv6-address* [**via** *mgmt-name*]

ipv6 host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ipv6-address*

no ipv6 host [**oob**] *host-name* [*telnet-port*] *ipv6-address* [**via** *mgmt-name*]

no ipv6 host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ipv6-address*

Parameter Description

oob: Configures out-of-band management.

vrf *vrf-name*: Configures a VRF instance.

host-name: Host name of a device.

ipv6-address: IPv6 address of a device.

via *mgmt-name*: Specifies the outbound management interface of packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the static mapping between host name www.test6.com and IPv6 address 2001:0DB8:700:20:1::12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 host www.test6.com 2001:0DB8:700:20:1::12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show hosts**
- **clear host**

1.7 ip dns proxy cache

Function

Run the **ip dns proxy cache** command to enable the function of caching dynamic entries on the DNS proxy.

Run the **no** form of this command to disable this feature.

The function of caching dynamic entries on the DNS proxy is enabled by default.

Syntax

ip dns proxy cache

no ip dns proxy cache

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When processing a request packet from the DNS client, the DNS proxy searches for the domain name-IP mapping in the local cache first. If the required domain name-IP mapping is found, the DNS proxy directly returns it to the client. If the required domain name-IP mapping is not found, the DNS resolver searches an external DNS server for the IP address mapped to the domain name and returns a reply packet to the client.

Examples

The following example disables the function of caching dynamic entries on the DNS proxy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dns proxy cache
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip dns proxy enable

1.8 ip dns proxy enable

Function

Run the **ip dns proxy enable** command to enable the DNS proxy function.

Run the **no** form of this command to disable this feature.

DNS proxy is disabled by default.

Syntax

ip dns proxy enable

no ip dns proxy enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

DNS proxy is generally deployed on the front-end egress gateway between a DNS server and a PC, and acts as a proxy of the DNS server to process users' DNS domain name resolution requests.

Examples

The following example disables the DNS proxy function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dns proxy enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip dns proxy host

Function

Run the **ip dns proxy host** command to configure a static mapping between a host name and an IP address on the DNS proxy.

Run the **no** form of this command to remove this configuration.

No static mapping between a host name and an IP address is configured on the DNS proxy by default.

Syntax

ip dns proxy host *host-name* { *ipv4-address* | *ipv6-address* }

no ip dns proxy host *host-name* { *ipv4-address* | *ipv6-address* }

Parameter Description

host-name: Host name of a device.

ipv4-address: IPv4 address of a device.

Ipv6-address: IPv6 address of a device.

Command Modes

Global configuration mode

Usage Guidelines

N/A

Examples

The following example configures a static mapping between host name www.test.com and IP address 192.168.5.243 on the DNS proxy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dns proxy host www.test.com 192.168.5.243
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **clear dns proxy host**
- **show dns proxy hosts**

1.10 ip dns proxy nameserver

Function

Run the **ip dns proxy nameserver** command to configure the IP address of a DNS server on the DNS proxy.

Run the **no** form of this command to remove this configuration.

No DNS server is configured on the DNS proxy by default.

Syntax

ip dns proxy nameserver { *ipv4-address* | *ipv6-address* }

no ip dns proxy nameserver [*ipv4-address* | *ipv6-address*]

Parameter Description

ipv4-address: IPv4 address of a DNS server.

ipv6-address: IPv6 address of a DNS server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Each time this command is run, the device will add one DNS server. When a domain name cannot be obtained from the first server, the device tries to send a DNS request to subsequent servers until it receives a correct reply.

The system supports up to six DNS servers. If the *ipv4-address* or *ipv6-address* parameter is specified when you delete a DNS server, only the specified server will be deleted. Otherwise, the IP addresses of all DNS servers will be deleted.

Examples

The following example sets the IPv4 address of a DNS server to 192.168.5.134 on the DNS proxy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dns proxy nameserver 192.168.5.134
```

The following example sets the IPv6 address of a DNS server to 2001::1 on the DNS proxy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dns proxy nameserver 2001::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ip dns proxy port-range

Function

Run the **ip dns proxy port-range** command to configure the range of a port used for query in upper-level DNS servers.

Run the **no** form of this command to restore the default configuration.

The default port range is from 55000 to 58000.

Syntax

ip dns proxy port-range *port-min port-max*

no ip dns proxy port-range

Parameter Description

port-min: Minimum value of the port range. The value range is from 1025 to 65535. The default value is 55000.

port-max: Maximum value of the port range. The value range is from 1025 to 65535. The default value is 58000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to adjust the range of a port used for query in upper-level DNS servers.

If the port range is too small, the concurrent processing performance of the device is affected. On the contrary, if the port range is too large, excessive flow table entry resources will be occupied and the egress device needs to adjust the flow table restriction synchronously.

Examples

The following example configures the range of a port used for query in the upper-level DNS servers to 30000 to 35000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dns proxy port-range 30000 35000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip dns proxy ttl

Function

Run the **ip dns proxy ttl** command to configure the time to live (TTL) of the reply packet in response to a static entry.

Run the **no** form of this command to restore the default configuration.

The default TTL of the reply packet in response to a static entry is 3,600 seconds.

Syntax

ip dns proxy ttl *ttl*

no ip dns proxy ttl

Parameter Description

ttl: TTL of the reply packet in response to a static entry, in seconds. The value range is from 10 to 65535, and the default value is 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the TTL of the reply packet in response to a static entry to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dns proxy ttl 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show hosts

Function

Run the **show hosts** command to display the DNS configuration.

Syntax

show hosts [**vrf** *vrf-name* | **oob** [**via** *mgmt-name*]] [*host-name*]

Parameter Description

oob: Configures out-of-band management.

vrf *vrf-name*: Configures a VRF instance.

via *mgmt-name*: Specifies the outbound management interface of packets.

host-name: Specified domain name. If this parameter is not specified, all domain names will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the DNS configuration.

```
Hostname> enable
Hostname# show hosts
Name servers are:
192.168.5.134 static
Host             type         Address             TTL(sec)
switch           static      192.168.5.243          -
www.dnstest.com   dynamic     192.168.5.123          126
```

Table 1-1 Output Fields of the show hosts Command

Field	Description
Name servers	DNS servers.
Host	Domain name.

Field	Description
type	Resolution type. ● **static** indicates static resolution. ● **dynamic** indicates dynamic resolution.
Address	IP address mapped to a domain name.
TTL	TTL of a domain name/IP entry.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show dns proxy hosts

Function

Run the **show dns proxy hosts** command to display the entries on the DNS proxy.

Syntax

show dns proxy hosts

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all entries on the DNS proxy.

```
Hostname> enable
Hostname# show dns proxy hosts
proxy state: enable
Name servers are:
```

```
192.168.59.194
2.0.0.3
static host    max: 1024
static host   count: 1
cache domain    max: 5120
cache domain  count: 1
Host                                                    type          TTL(sec)
Address
www.Hostname.net                                           static        -
192.168.5.21
www.baidu.com                                            dynamic       109
163.177.151.110

163.177.151.109
```

Table 1-2 Output Fields of the show dns proxy hosts Command

Field	Description
proxy state	Functional status of a service.
Name servers	DNS servers.
static host max	Maximum number of supported static entries.
static host count	Number of static entries used.
cache domain max	Maximum number of dynamic entries.
cache domain count	Number of dynamic entries used.
Host	Domain name.
type	Resolution type. ● **static** indicates static resolution. ● **dynamic** indicates dynamic resolution.
Address	IP address mapped to a domain name.
TTL	TTL of a domain name/IP entry.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show dns proxy statistics

Function

Run the **show dns proxy statistics** command to display the DNS proxy packet statistics.

Syntax

show dns proxy statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays DNS proxy packets statistics.

```
Hostname> enable
Hostname# show dns proxy statistics
Receive client request packet counts : 0
Send to client reply packet counts   : 0
Send to server request packet counts : 0
Receive server reply packet counts   : 0
```

Table 1-3 Output Fields of the show dns proxy hosts Command

Field	Description
Receive client request packet counts	Number of received request packets from the DNS client.
Send to client reply packet counts	Number of response packets sent to the DNS client.
Send to server request packet counts	Number of request packets sent to the DNS server.
Receive server reply packet counts	Number of received response packets from the DNS server.
Deal timeout packet counts	Number of timeout DNS request timeout packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 IPv6 Basics Commands

Command	Function
clear ipv6 neighbors	Clear dynamically learned neighbor discovery (ND) entries.
ipv6 address	Configure an IPv6 address.
ipv6 address autoconfig	Enable IPv6 stateless address auto-configuration on an interface.
ipv6 icmp error-interval	Configure the transmission rate of other ICMPv6 error messages.
ipv6 enable	Enable the IPv6 protocol on an interface.
ipv6 gateway	Configure the IPv6 default gateway for a management interface.
ipv6 general-prefix	Configure an IPv6 general prefix.
ipv6 hop-limit	Configure the hop limit for unicast packets.
ipv6 icmp source	Configure a specified source address for sending ICMPv6 packets.
ipv6 mtu	Configure the MTU for IPv6 packets.
ipv6 nd cache interface-limit	Configure the maximum number of neighbor cache entries that can be learned by an interface.
ipv6 nd dad attempts	Configure the number of neighbor solicitation (NS) packets to be sent consecutively during duplicate address detection (DAD).
ipv6 nd dad learning enable	Enable an interface to learn ND entries via DAD NS packets.
ipv6 nd dad retry	Configure the DAD interval.
ipv6 nd log enable	Enable ND logging.
ipv6 nd log rate	Configure the ND logging rate.
ipv6 nd managed-config-flag	Configure the Managed address configuration flag bit in the RA packets.
ipv6 nd max-opt	Configure the number of ND options supported by the device.

ipv6 nd ns-interval	Configure the NS packet retransmission interval.
ipv6 nd other-config-flag	Configure the Other stateful configuration flag bit in the RA packets.
ipv6 nd prefix	Configure the address prefix to be contained in the RA packets.
ipv6 nd packet rate-statistics interval	Configure the interval for collecting ND packet rate statistics.
ipv6 nd ra dns server suppress	Configure RA packets not to carry the RDNSS option.
ipv6 nd ra dns server sequence	Configure the address of the DNS recursive query server in RA packets.
ipv6 nd ra dns search-list suppress	Configure RA packets not to carry the DNSSL option.
ipv6 nd ra dns search-list sequence	Configure the DNS suffix to be contained in an RA packet.
ipv6 nd ra-hoplimit	Configure the hop limit for RA packets to be sent by an interface.
ipv6 nd ra-interval	Configure the interval for sending RA packets on an interface.
ipv6 nd ra-lifetime	Configure the router lifetime in RA packets to be sent on an interface.
ipv6 nd ra-mtu	Configure the MTU for RA packets to be sent on an interface.
ipv6 nd ra-url	Configure the Uniform Resource Locator (URL) for RA packets to be sent on an interface.
ipv6 nd ra-url	Configure the URL option type value for RA packets to be sent.
ipv6 nd reachable-time	Configure the duration in which the device considers a neighbor reachable.
ipv6 nd resolve vlan	Configure the device to actively send NS packets to a specific sub VLAN in a super VLAN.
ipv6 nd stale-time	Configure the duration in which a neighbor keeps in stale state.
ipv6 nd suppress-auth-vlan-ns	Configure an interface not to send NS packets to an authenticated VLAN.
ipv6 nd suppress-ra	Configure an interface not to send RA packets.

ipv6 nd unresolved	Configure the maximum number of unresolved ND entries.
ipv6 neighbor	Configure a static neighbor entry.
ipv6 ns-linklocal-src	Configure the link-local address as the source address for sending NS packets.
ipv6 redirects	Enable the ICMPv6 redirection function.
ipv6 source-route	Configure the device to forward IPv6 packets carrying the routing header.
local-proxy-nd enable	Enable the local ND proxy function on an interface.
show ipv6 address	Display the information about an IPv6 address.
show ipv6 general-prefix	Display the prefix information in a general prefix.
show ipv6 interface	Display the information about an IPv6 interface.
show ipv6 nd	Display the statistics on IPv6 ND packets.
show ipv6 neighbors	Display IPv6 neighbor tables.
show ipv6 neighbors statistics	Display the statistics on IPv6 neighbor tables.
show ipv6 packet statistics	Display the statistics on IPv6 packets.
show ipv6 raw-socket	Displays all IPv6 raw sockets.
show ipv6 routers	Display neighbor router information and RA packets.
show ipv6 sockets	Display all IPv6 raw sockets.
show ipv6 udp	Display all IPv6 UDP sockets.
show ipv6 udp statistics	Display the statistics on IPv6 UDP sockets.

1.1 clear ipv6 neighbors

Function

Run the **clear ipv6 neighbors** command to clear dynamically learned neighbor discovery (ND) entries.

Syntax

clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-type interface-number*]

Parameter Description

vrf *vrf-name*: Specifies the name of a virtual routing and forwarding (VRF) instance. If this parameter is not specified, it indicates the public network instance.

oob: Clears all the ND entries dynamically learned via the Neighbor Discovery Protocol (NDP) on the management interface.

interface-type interface-number: Interface type and interface number. After this parameter is specified, the dynamic ND entries of a specified interface will be deleted.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Static ND entries will not be cleared.

When this command is run in gateway authentication mode, the device will not delete dynamic ND entries in authenticated VLANs.

Examples

The following example clears all the dynamically learned ND entries.

```
Hostname> enable
Hostname# clear ipv6 neighbors
```

The following example clears all the dynamically learned ND entries on the management interface.

```
Hostname> enable
Hostname# clear ipv6 neighbors oob
```

The following example clears all the dynamically learned ND entries on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ipv6 neighbors gigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ipv6 address

Function

Run the **ipv6 address** command to configure an IPv6 address.

Run the **no** form of this command to remove this configuration.

No IPv6 address is configured by default.

Syntax

ipv6 address *ipv6-address*/*prefix-length*

no ipv6 address *ipv6-address*/*prefix-length*

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

no ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

ipv6 address *prefix-name sub-bits*/*prefix-length* [**eui-64**]

no ipv6 address *prefix-name sub-bits*/*prefix-length* [**eui-64**]

no ipv6 address

Parameter Description

ipv6-address: IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

ipv6-prefix: IPv6 address prefix, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

prefix-length: Length of an IPv6 address prefix, that is, the network address part in an IPv6 address.

prefix-name: Name of a general prefix. This specified general prefix is used to generate an interface address.

sub-bits: Subprefix bits and host bits. This value is combined with the prefix in the general prefix to generate an interface address. This value must be represented in the form of colon hexadecimal notation as documented in RFC 4291.

eui-64: Indicates that the generated IPv6 address consists of the configured address prefix and 64-bit interface ID.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If an IPv6 interface is created and the link is in up state, the system automatically generates a link-local address for this interface.

The IPv6 address of an interface can also be generated using the general prefix mechanism. That is, IPv6 address = General prefix + Sub prefix + Host bits. The general prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery (PD) function of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client. For details, see "Configuring DHCPv6" in the *IP Configuration Guide*. The sub prefix + host bits are specified by the *sub-bits/prefix-length* parameter in this command.

Caution

- If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, no IPv6 address can be configured for this interface. You can configure an IPv6 address for this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.
- Anycast addresses (such as 1000:1::100/120 and 1000::/64) cannot be configured as interface IPv6 addresses. Exceptionally, anycast addresses with a subnet prefix of 127 or greater can be configured.

Examples

The following example sets the IPv6 address to 2001:1::1/64 for port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
```

The following example configures an address for port GigabitEthernet 0/1 by using the general prefix my-prefix and setting the subprefix bits and host bits to 0:0:0:7272::72/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix 0:0:0:7272::72/64
```

Note

Assume that the prefix configured by using the general prefix my-prefix is 2001:1111:2222::/48. The generated interface IPv6 address is 2001:1111:2222:7272::72/64.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 general-prefix**
- **show ipv6 address**
- **show ipv6 interface**

1.3 ipv6 address autoconfig

Function

Run the **ipv6 address autoconfig** command to enable IPv6 stateless address auto-configuration on an interface.

Run the **no** form of this command to disable this feature.

The IPv6 stateless address auto-configuration is disabled on an interface by default.

Syntax

ipv6 address autoconfig [**default**]

no ipv6 address autoconfig

Parameter Description

default: Generates a default route for the address that is automatically configured under stateless conditions. Only one L3 interface on a device can use the **default** keyword. No default route is generated by default.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Caution

If an interface is bound to a multiprotocol VRF instance not configured with the IPv6 address family, the IPv6 stateless address auto-configuration cannot be enabled on the interface. You can enable the IPv6 stateless address auto-configuration on this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.

Stateless address auto-configuration means that, when a device receives a router advertisement (RA) packet, an interface address in EUI-64 format can be automatically generated using prefix information in the RA packet.

If the RA packet received contains **other-config-flag**, the interface will get other configuration parameters such as the IPv6 address of the domain name system (DNS) server and the IPv6 address of the Network Time Protocol (NTP) server through DHCPv6.

Examples

The following example enables the IPv6 stateless address auto-configuration on port GigabitEthernet 0/1 and generates a default route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address autoconfig default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 address**
- **show ipv6 interface**

1.4 ipv6 icmp error-interval

Function

Run the **ipv6 icmp error-interval** command to configure the transmission rate of other ICMPv6 error messages.

Run the **no** form of this command to restore the default configuration.

Ten ICMPv6 error messages are transmitted in 100 ms by default.

Syntax

ipv6 icmp error-interval [**too-big**] *interval* [*bucket-size*]

no ipv6 icmp error-interval [**too-big**] *interval* [*bucket-size*]

Parameter Description

too-big: Specifies the transmission rate of ICMPv6 Packet Too Big messages.

interval: Refresh cycle of a token bucket, in ms. The value range is from 0 to 2147483647, and the default value is **100**. If the value is **0**, the transmission rate of ICMPv6 error messages is not restricted.

bucket-size: Number of tokens contained in a token bucket. The value range is from 1 to 200, and the default value is **10**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent denial of service (DoS) attacks, you can use the token bucket algorithm to restrict the transmission rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 maximum transmission unit (MTU) of the outbound interface, the router discards this IPv6 packet and sends an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used for IPv6 PMTUD. When there are too many other

ICMPv6 error messages, the ICMPv6 Packet Too Big message cannot be sent, causing the failure of IPv6 PMTUD. Therefore, you are advised to restrict the transmission rate of ICMPv6 Packet Too Big messages and other ICMPv6 error packets separately.

Note

Although ICMPv6 Redirect packets are not a type of ICMPv6 error messages, the device limit the transmission rate of other ICMPv6 error messages, together with ICMPv6 Redirect packets.

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the transmission rate is set to 1 packet per 5 milliseconds, two ICMP error packets are actually sent per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the transmission rate is set to 3 packets per 15 milliseconds, two ICMP error packets are actually sent per 10 milliseconds.

Examples

The following example sets the transmission rate of ICMPv6 Packet Too Big messages to 100 pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the transmission rate of other ICMPv6 error messages to 10 pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp error-interval 1000 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 enable

Function

Run the **ipv6 enable** command to enable the IPv6 protocol on an interface.

Run the **no** form of this command to disable this feature.

The IPv6 protocol is disabled on an interface by default.

Syntax

ipv6 enable

no ipv6 enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

There are two ways to enable the IPv6 function on an interface:

- Configure the **ipv6 enable** command on an interface;
- Directly configure an IPv6 address on an interface.

Caution

If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, IPv6 cannot be enabled on this interface. You can enable IPv6 on this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.

If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface and cannot be disabled even when you run the **no ipv6 enable** command.

Examples

The following example enables the IPv6 function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 address**
- **show ipv6 interface**

1.6 ipv6 gateway

Function

Run the **ipv6 gateway** command to configure the IPv6 default gateway for a management interface.

No IPv6 default gateway is configured for a management interface by default.

Syntax

ipv6 gateway *ipv6-address*

Parameter Description

ipv6-address: IPv6 default gateway address of a management interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The type of a management interface is MGMT and the interface number is fixed to 0.

Examples

The following example sets the IPv6 default gateway of a management interface to 2001:1::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-MGMT 0)# ipv6 gateway 2001:1::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.7 ipv6 general-prefix

Function

Run the **ipv6 general-prefix** command to configure an IPv6 general prefix.

Run the **no** form of this command to remove this configuration.

No IPv6 general prefix is configured by default.

Syntax

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter Description

prefix-name: Name of a general prefix.

ipv6-prefix/prefix-length: Network prefix value and prefix length of the general prefix.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A general prefix can facilitate network numbering. The prefix defined in a general prefix can be referenced by a longer specific prefix. When the general prefix changes, the specific prefixes that reference the general prefix will change accordingly. When a network ID changes, only the general prefix needs to be changed.

A general prefix can contain several prefixes.

Examples

The following example configures a general prefix named my-prefixIPv6, with the network prefix value of 2001:1111:2222::/48.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 general-prefix**

1.8 ipv6 hop-limit

Function

Run the **ipv6 hop-limit** command to configure the hop limit for unicast packets.

Run the **no** form of this command to restore the default configuration.

The default hop limit for unicast packets is 64.

Syntax

ipv6 hop-limit *hop*

no ipv6 hop-limit

Parameter Description

hop: Hop limit value. The value range is from 1 to 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is effective to unicast packets only.

Examples

The following example sets the hop limit for unicast packets to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 hop-limit 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ipv6 icmp source

Function

Run the **ipv6 icmp source** command to configure a specified source address for sending ICMPv6 packets.

Run the **no** form of this command to restore the default configuration.

No specified source address is configured for ICMPv6 packets by default.

Syntax

ipv6 icmp source [**vrf** *vrf-name*] *ipv6-address*

no ipv6 icmp source

Parameter Description

vrf *vrf-name*: Specifies a VRF instance.

ipv6-address: IPv6 address used to send packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In a network with a large number of IPv6 addresses configured, it is complex for receivers to recognize the device, from which an ICMPv6 packet is sent. To simplify the judgment, you can configure a specified source address for ICMPv6 packets. You can choose a specified address, like the address of the loopback interface, as the source address of ICMPv6 packets.

Examples

The following example sets the source address of ICMPv6 reply packets to 1001::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 icmp souce 1001::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 mtu

Function

Run the **ipv6 mtu** command to configure the MTU for IPv6 packets.

Run the **no** form of this command to restore the default configuration.

The MTU value of IPv6 packets is the same as the value configured by running the **mtu** command on an interface by default.

Syntax

ipv6 mtu *mtu*

no ipv6 mtu

Parameter Description

mtu: MTU of IPv6 packets. The value range is from 1280 to 1500.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the size of an IPv6 packet exceeds the IPv6 MTU size, the packet will be fragmented.

For all devices in the same physical network segment, the IPv6 MTU of interconnected interfaces must be the same.

Examples

The following example sets the IPv6 MTU of port gigabitEthernet 0/1 to 1400 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.11 ipv6 nd cache interface-limit

Function

Run the **ipv6 nd cache interface-limit** command to configure the maximum number of neighbor cache entries that can be learned by an interface.

Run the **no** form of this command to restore the default configuration.

The number of neighbor cache entries that can be learned by an interface is not limited by default.

Syntax

ipv6 nd cache interface-limit *limit*

no ipv6 nd cache interface-limit

Parameter Description

limit: Maximum number of neighbor cache entries that can be learned by an interface, including static and dynamic neighbor cache entries. The value range is from 1 to 8000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Restricting the number of neighbor cache entries that can be learned by an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of neighbor cache entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the neighbor cache entries learned by the current interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Examples

The following example sets the maximum number of neighbor cache entries that can be learned by port GigabitEthernet 0/1 to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ipv6 nd dad attempts

Function

Run the **ipv6 nd dad attempts** command to configure the number of neighbor solicitation (NS) packets to be sent consecutively during duplicate address detection (DAD).

Run the **no** form of this command to restore the default configuration.

The default number of NS packets to be sent consecutively during DAD is **1**.

Syntax

ipv6 nd dad attempts *attempts*

no ipv6 nd dad attempts

Parameter Description

attempts: Number of NS packets. The value range is from 0 to 600, and the default value is **1**. When the parameter is set to **0**, DAD is not enabled for the IPv6 address of this interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You need to enable DAD before configuring an IPv6 address for an interface. At this moment, the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address is an EUI-64 ID, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface. At the time, you must configure a new address for the interface and disable and then enable the interface to start DAD again.

When an interface changes from the down state to the up state, DAD is re-enabled on this interface.

Examples

The following example configures three NS packets to be sent consecutively during DAD on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd dad attempts 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.13 ipv6 nd dad learning enable

Function

Run the **ipv6 nd dad learning enable** command to enable an interface to learn ND entries via DAD NS packets.

Run the **no** form of this command to restore the default configuration.

The function of learning ND entries via DAD NS packets by an interface is disabled by default.

Syntax

ipv6 nd dad learning enable

no ipv6 nd dad learning enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this function is configured on an interface, the interface will create an ND entry in stale state when receiving a DAD NS packet.

By default, a general interface is disabled to learn ND entries via DAD NS packets but interfaces in a super VLAN are allowed to do so.

Examples

The following example enables the function of learning ND entries via DAD NS packets on VLAN 1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# ipv6 nd dad learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 nd dad retry

Function

Run the **ipv6 nd dad retry** command to configure the DAD interval.

Run the **no** form of this command to restore the default configuration.

The default DAD interval is 60s.

Syntax

ipv6 nd dad retry *retry*

no ipv6 nd dad retry

Parameter Description

retry: DAD interval after an address conflict is detected, in seconds. The value range is from 0 to 7200. If this value is set to **0**, the repeated DAD is disabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You need to enable DAD before configuring an IPv6 address on an interface. If an address conflict is detected, the device will not receive IPv6 packets destined for this address.

With this command, the software will conduct DAD again on the conflicting address at the configured interval. If no address conflict is detected, this address can be normally used.

Examples

The following example sets the DAD interval to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd dad retry 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ipv6 nd log enable

Function

Run the **ipv6 nd log enable** command to enable ND logging.

Run the **no** form of this command to disable this feature.

ND logging is disabled by default.

Syntax

ipv6 nd log enable

no ipv6 nd log enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, system logs will be printed for ND packets (including RS, RA, NS, and NA packets) received and sent by the device.

Examples

The following example enables ND logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd log enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ipv6 nd log rate

Function

Run the **ipv6 nd log rate** command to configure the ND logging rate.

Run the **no** form of this command to restore the default configuration.

Twenty ND logs are printed per minute by default.

Syntax

ipv6 nd log rate *rate*

no ipv6 nd log rate

Parameter Description

rate: ND logging rate, in entries/minute. The value range is from 0 to 65535. The default value is **20**, that is, 20 logs are printed per minute. The rate is not limited when *rate* is set to **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables ND logging and sets the rate to 200 logs per minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd log enable
Hostname(config)# ipv6 nd log rate 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ipv6 nd managed-config-flag

Function

Run the **ipv6 nd managed-config-flag** command to configure the **Managed address configuration** flag bit in the RA packets.

Run the **no** form of this command to remove this configuration.

The **Managed address configuration** flag bit in the RA packets is not configured by default.

Syntax

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The settings of the **Managed address configuration** flag bit determine whether a host receiving this RA packet obtains an address through stateful address auto-configuration. If this flag bit is configured, an address will be obtained through stateful address auto-configuration. Otherwise, an address will not be obtained through stateful address auto-configuration.

Examples

The following example configures the **Managed address configuration** flag bit in the RA packets on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd managed-config-flag
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 interface

1.18 ipv6 nd max-opt

Function

Run the **ipv6 nd max-opt** command to configure the number of ND options supported by the device.

Run the **no** form of this command to restore the default configuration.

The device supports 10 ND options by default.

Syntax

ipv6 nd max-opt *option*

no ipv6 nd max-opt

Parameter Description

option: Number of supported options. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of ND options that can be processed by the device, such as the source link-layer address option, MTU option, redirection option, and prefix option.

Examples

The following example sets the maximum number of ND options supported by the device to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd max-opt 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ipv6 nd ns-interval

Function

Run the **ipv6 nd ns-interval** command to configure the NS packet retransmission interval.

Run the **no** form of this command to restore the default configuration.

The default NS packet retransmission interval of an interface is not specified when the interval is filled in the RA packets, and 1000 ms when it is used to control the interval for the device to transmit NS packets.

Syntax

ipv6 nd ns-interval *interval*

no ipv6 nd ns-interval

Parameter Description

interval: NS packet retransmission interval, in milliseconds. The value range is from 1000 to 4294967295, and the default value is **1000**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The configured value is advertised in an RA packet and is also used on the device.

Examples

The following example sets the NS packet retransmission interval to 2s on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd ns-interval 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.20 ipv6 nd other-config-flag

Function

Run the **ipv6 nd other-config-flag** command to configure the **Other stateful configuration** flag bit in the RA packets.

Run the **no** form of this command to remove this configuration.

No **Other stateful configuration** flag bit in the RA packets is configured by default.

Syntax

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the **Other stateful configuration** flag bit is set, the flag bit in the RA packets sent from the device is set to 1. After a host receives this flag bit, it obtains other information except the IPv6 address through DHCPv6 for auto-configuration. When **Managed address configuration** is set, **Other stateful configuration** is also set by default.

Examples

The following example configures the **Other stateful configuration** flag bit in the RA packets on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd other-config-flag
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.21 ipv6 nd prefix

Function

Run the **ipv6 nd prefix** command to configure the address prefix to be contained in the RA packets.

Run the **no** form of this command to remove this configuration.

By default, the prefix in an RA packet on an interface is the prefix configured using the **ipv6 address** command on the interface.

Syntax

ipv6 nd prefix { *ipv6-prefix*/*prefix-length* | **default** } [*valid-lifetime* { **infinite** | *preferred-lifetime* } | **at** *valid-date preferred-date* | **infinite** { **infinite** | *preferred-lifetime* }] [**no-advertise**] | [[**off-link**] [**no-autoconfig**] | **pool** *pool-name* | **preference** { **high** | **medium** | **low** } [**proxy**]]

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** }

Parameter Description

ipv6-prefix/*prefix-length*: IPv6 address prefix and prefix length, which must comply with the address representation format in RFC 4291.

valid-lifetime: Lifetime of a prefix considered valid by a host after the host receives the prefix in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **2592000** seconds, that is, 30 days.

preferred-lifetime: Preferred lifetime of a prefix considered valid by a host after the host receives the prefix in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **604800** seconds, that is, 7 days.

valid-date preferred-date: End time, before which the prefix in an RA packet is considered valid. The end time uses the format of dd+mm+yyyy+hh+mm.

preferred-date: Preferred end time, before which the prefix in an RA packet is considered valid. The end time uses the format of dd+mm+yyyy+hh+mm.

infinite: Indicates that it is permanently valid.

default: Configures the default parameter settings.

no-advertise: Indicates that the prefix is not advertised by a router.

off-link: If the prefix of the destination address in an IPv6 packet sent by a host matches the configured prefix, the destination address is considered on the same link (on-link) and directly reachable. This parameter indicates that this prefix is not used for on-link determination.

no-autoconfig: Indicates that the prefix in an RA packet received by a host cannot be used for address auto-configuration.

pool *pool-name*: Configures a specific prefix pool to be bound to an interface to ensure that different IPv6 prefixes are allocated to different users.

preference: Sets the routing priority. The value is **high**, **medium**, or **low**. The default value is **medium**.

proxy: Enables the ND proxy based on the prefix.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command can be used to configure parameters for each prefix individually and determine whether to advertise a prefix.

By default, the prefix in an RA packet on an interface is the prefix configured using the **ipv6 address** command on the interface. To add other prefixes, run this command.

The **ipv6 nd prefix default** command is used to configure the default parameters on this interface. That is, if no parameter is specified when a prefix is added, the parameters configured using the **ipv6 nd prefix default** command will be used as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, the use of the **ipv6 nd prefix default** command will not modify the configuration specified for a prefix, but only modify the configuration of a prefix that fully uses default parameter configurations.

The value of **at** *valid-date preferred-date* can be specified for a prefix in two ways: (1) specifying a fixed time length for each prefix in an RA packet; (2) specifying the end time. The valid lifetime of the prefix in each RA packet decreases till it becomes 0.

If no parameter is specified when a prefix is added, the default parameter configurations will apply. That is, this prefix is also not available for address auto-configuration.

Examples

The following example configures the prefix of an address included in an RA packet to 2001::/64 and valid lifetime to 2,592000 seconds on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example configures the prefix of an address included in an RA packet not to be used for address auto-configuration on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd default no-autoconfig
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.22 ipv6 nd packet rate-statistics interval

Function

Run the **ipv6 nd packet rate-statistics interval** command to configure the interval for collecting ND packet rate statistics.

Run the **no** form of this command to restore the default configuration.

The ND packet rate statistics collection is disabled by default.

Syntax

ipv6 nd packet rate-statistics interval *interval*

no ipv6 nd packet rate-statistics interval

Parameter Description

interval: Sampling interval, in seconds. The value range is from 60 to 86400.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This configuration can modify the interval for collecting ND packet rate statistics. For example, if the interval is set to 60, the ND packet rate is calculated once every 60 seconds.

Examples

The following example sets the interval for collecting ND packet rate statistics to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd packet rate-statistics interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 nd

1.23 ipv6 nd ra dns server suppress

Function

Run the **ipv6 nd ra dns server suppress** command to configure RA packets not to carry the RDNSS option.

Run the **no** form of this command to remove this configuration.

An RA packet does not carry the RDNSS option by default.

Syntax

ipv6 nd ra dns server suppress

no ipv6 nd ra dns server suppress

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The RDNSS option can provide IPv6 terminals with the address of the DNS recursive query server.

Examples

The following example configures RA packets to carry the RDNSS option on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns server suppress
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 nd

1.24 ipv6 nd ra dns server sequence

Function

Run the **ipv6 nd ra dns server sequence** command to configure the address of the DNS recursive query server in RA packets.

Run the **no** form of this command to remove this configuration.

The address of the DNS recursive query server in RA packets is not configured by default.

Syntax

ipv6 nd ra dns server *ipv6-address* { *valid-lifetime* | **infinite** } **sequence** *number*

no ipv6 nd ra dns server *ipv6-address* { *valid-lifetime* | **infinite** } **sequence** *number*

Parameter Description

ipv6-address: IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.

valid-lifetime: Lifetime of the RDNSS option considered valid by a host after the host receives the RDNSS option in an RA packet, in seconds. The value range is from 0 to 4294967295. When the parameter is set to **0**, the RDNSS option is no longer used.

infinite: Indicates that it is permanently valid.

sequence *number*: Indicates a sequence number, which represents the serial number of the same RDNSS option in an RA packet. The value range is from 0 to 7.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Only one option can be configured with the same sequence number under the same interface, and the same IPv6 address can only be used by one sequence number.

When configured, the RDNSS options are advertised through RA packet, and are organized in the descending order of sequence numbers.

Examples

The following example configures RA packets to carry the RDNSS options, sets the address of the DNS recursive query server to 2018::1 and be permanently valid, and sets the sequence number to 0 on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns server suppress
Hostname(config-if-VLAN 1)# ipv6 nd ra dns server 2018::1 infinite sequence 0
Hostname(config-if-VLAN 1)# ipv6 nd ra dns server 2020::1 1000 sequence 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 nd**

1.25 ipv6 nd ra dns search-list suppress

Function

Run the **ipv6 nd ra dns search-list suppress** command to configure RA packets not to carry the DNSSL option.

Run the **no** form of this command to remove this configuration.

RA packets do not carry the DNSSL option by default.

Syntax

ipv6 nd ra dns search-list suppress

no ipv6 nd ra dns search-list suppress

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The DNSSL option can provide IPv6 terminals with a search list of DNS domain names.

Examples

The following example configures RA packets to carry the DNSSL option on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns search-list suppress
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

show ipv6 nd

1.26 ipv6 nd ra dns search-list sequence

Function

Run the **ipv6 nd ra dns search-list sequence** command to configure the DNS suffix to be contained in an RA packet.

Run the **no** form of this command to remove this configuration.

The DNS suffix to be contained in an RA packet is not configured by default.

Syntax

ipv6 nd ra dns search-list *ipv6-domain-name* { *valid-lifetime* | **infinite** } **sequence** *number*

no ipv6 nd ra dns search-list *ipv6-domain-name* { *valid-lifetime* | **infinite** } **sequence** *number*

Parameter Description

ipv6-domain-name: DNS suffix. It is a string of 1 to 64 characters.

valid-lifetime: Lifetime of the DNSSL option considered valid by a host after the host receives the DNSSL option in an RA packet, in seconds. The value range is from 0 to 4294967295. The default value is **1800**. When the value is set to **0**, it is no longer used.

infinite: Indicates that it is permanently valid.

number: Indicates a sequence number, which represents the serial number of the same DNSSL option in an RA packet.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Only one domain name option can be configured with the same sequence number under the same interface, and the same domain name can only be used by one sequence number.

When configured, the DNSSL option is advertised through RA packets, and are organized in the descending order of sequence numbers.

Examples

The following example enables RA packets to carry the DNSSL option, sets the DNS suffix to text.com.cn, configures the suffix to be permanently valid, and sets the sequence number to 0 on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface vlan 1
Hostname(config-if-VLAN 1)# no ipv6 nd ra dns search-list suppress
Hostname(config-if-VLAN 1)# ipv6 nd ra dns search-list test.com.cn infinite sequence
0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 nd**

1.27 ipv6 nd ra-hoplimit

Function

Run the **ipv6 nd ra-hoplimit** command to configure the hop limit for RA packets to be sent by an interface.

Run the **no** form of this command to restore the default configuration.

The default hop limit of RA packets is 64.

Syntax

ipv6 nd ra-hoplimit *hoplimit*

no ipv6 nd ra-hoplimit

Parameter Description

hoplimit: Hop limit of RA packets. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the hop limit of RA packets to 110 on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.28 ipv6 nd ra-interval

Function

Run the **ipv6 nd ra-interval** command to configure the interval for sending RA packets on an interface.

Run the **no** form of this command to restore the default configuration.

The default interval for sending RA packets on an interface is 600s.

Syntax

ipv6 nd ra-interval { *interval* | **min-max** *min-interval max-interval* }

no ipv6 nd ra-interval

Parameter Description

interval: Interval for sending RA packets, in seconds. The value range is from 3 to 1800.

min-max: Sets the maximum and minimum intervals for sending RA packets.

min-interval: Minimum interval for sending RA packets, in seconds. The value range is from 3 to 1800.

max-interval: Maximum interval for sending RA packets, in seconds. The value range is from 4 to 1800.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When a device acts as a default routing device, the configured interval value cannot be greater than the lifetime of a router.

In addition, to prevent network bandwidth from being consumed by other devices sending RA packets at the same time on the link, the actual interval will fluctuate around this value by ±20%.

If **min-max** is specified, then the actual interval will be randomly selected between the minimum and maximum values.

Examples

The following example sets the interval for sending RA packets to 110 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval 110
```

The following example sets the interval for sending RA packets to a value in the range of 110 seconds to 120 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval min-max 110 120
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.29 ipv6 nd ra-lifetime

Function

Run the **ipv6 nd ra-lifetime** command to configure the router lifetime in RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

The default router lifetime in RA packets to be sent on an interface is 1800 seconds.

Syntax

ipv6 nd ra-lifetime *lifetime*

no ipv6 nd ra-lifetime

Parameter Description

lifetime: Lifetime of a device acting as a default device of this interface, in seconds. The value range is from 0 to 9000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The router lifetime (**Ra-lifetime**) field exists in each RA packet. This value indicates the amount of time that a host in the link where the interface is located can use the device as the default device. If this parameter is set to **0**, the device is no longer used as the default device. If this parameter is set to a non-zero value, this value must be greater than or equal to the interval for sending RA packets (**Ra-interval**).

Examples

The following example sets the lifetime in RA packets to 2000 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-lifetime 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.30 ipv6 nd ra-mtu

Function

Run the **ipv6 nd ra-mtu** command to configure the MTU for RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

The default MTU of RA packets is the IPv6 MTU value of a network interface.

Syntax

ipv6 nd ra-mtu *ra-mtu*

no ipv6 nd ra-mtu

Parameter Description

ra-mtu: Value of the MTU field in an RA packet, in bytes. The value range is from 0 to 1500.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If this parameter is set to **0**, an RA packet does not carry the MTU option.

Examples

The following example sets the MTU of RA packets to be sent to 1400 bytes on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-mtu 1400
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.31 ipv6 nd ra-url

Function

Run the **ipv6 nd ra-url** command to configure the Uniform Resource Locator (URL) for RA packets to be sent on an interface.

Run the **no** form of this command to restore the default configuration.

No URL is configured for RA packets by default.

Syntax

ipv6 nd ra-url [*ra-url*]

no ipv6 nd ra-url

Parameter Description

ra-url: URL of an RA packet. It is a string of 1 to 255 characters in a standard URL format.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the URL address of RA packets to be sent to www.test.com on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1) # ipv6 nd ra-url www.test.com
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.32 ipv6 nd ra-url

Function

Run the **ipv6 nd ra-url** command to configure the URL option type value for RA packets to be sent.

Run the **no** form of this command to restore the default configuration.

No URL option type value is configured for RA packets to be sent by default.

Syntax

ipv6 nd ra-url *type*

no ipv6 nd ra-url

Parameter Description

type: URL option type value of an RA packet. The value range is from 140 to 254, and should not be duplicate with a known type definition.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the URL option type value of RA packets to be sent to 234.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd ra-url 234
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 ipv6 nd reachable-time

Function

Run the **ipv6 nd reachable-time** command to configure the duration in which the device considers a neighbor reachable.

Run the **no** form of this command to restore the default configuration.

The default duration in which the device considers a neighbor reachable is 30000 ms (30s).

Syntax

ipv6 nd reachable-time *time*

no ipv6 nd reachable-time

Parameter Description

time: Duration in which the device considers a neighbor reachable, in milliseconds. The value range is from 0 to 3600000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

A device detects unreachable neighbors based on the configuration. A shorter duration indicates that the device detects unreachable neighbors more quickly but more network bandwidth and device resources will be consumed. Therefore, you are not advised to set the duration to a very small value.

The configured value is advertised in an RA packet and is also used on the device. If the value is **0**, the duration is not specified on the device and the default value is used.

Examples

The following example sets the duration in which a neighbor is considered reachable to 1000 seconds on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd reachable-time 1000000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.34 ipv6 nd resolve vlan

Function

Run the **ipv6 nd resolve vlan** command to configure the device to actively send NS packets to a specific sub VLAN in a super VLAN.

Run the **no** form of this command to disable this feature.

Run **default** form of this command to restore the default configuration.

The device is not configured to actively send NS packets to a specific sub VLAN in a super VLAN by default.

Syntax

ipv6 nd resolve vlan { *vlan-list* | **none** }

no ipv6 nd resolve vlan { *vlan-list* | **none** }

default ipv6 nd resolve vlan

Parameter Description

vlan-list: Sub VLAN segment, to which the device actively sends NS packets in the Super VLAN. After this parameter is configured, NS requests are sent to these VLAN lists only. The start and end VLANs in a sub VLAN segment are connected by a hyphen (-), and multiple sub VLAN segments are separated by commas (,), for example, 1, 3-5.

none: Indicates that no NS packet will be sent to any sub VLAN in a super VLAN.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

If there are many sub VLANs in a super VLAN, when actively broadcasting and resolving ND requests, the device will send NS packets to the entire super VLAN by default, and the packets will be replicated in large quantities, which will affect the performance of the device.

Most terminals (such as PCs or servers) request the ND tables of the gateway before accessing the network. Therefore, there is no need to actively send NS packets to the sub VLANs where these terminals reside. For dumb terminals (that do not actively send NA packets), this command can be deployed in the VLAN segment specified in *vlan-list*, to enable the device to actively send NS packets to these VLANs in an effort to generate ND entries with reachable state.

Caution

If an authentication-exempt VLAN is configured and the authentication-exempt VLAN is not in the VLAN list configured by running the **ipv6 nd resolve vlan** command, NS packets will not be actively broadcast to the authentication-exempt VLAN.

Examples

The following example configures the device to actively send NS packets to specific sub VLANs 10-20 and 25-30 in a super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd resolve vlan 10-20, 25-30
```

The following example configures the device not to send NS packets to any sub VLAN in a super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd resolve vlan none
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 ipv6 nd stale-time

Function

Run the **ipv6 nd stale-time** command to configure the duration in which a neighbor keeps in stale state.

Run the **no** form of this command to restore the default configuration.

The default duration in which a neighbor keeps in stale state is 3600s.

Syntax

ipv6 nd stale-time *time*

no ipv6 nd stale-time

Parameter Description

time: Duration in which a neighbor keeps in stale state, in seconds. The value range is from 0 to 86400.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

This command can be used to modify the duration of the stale state. After the duration expires, neighbor unreachability detection (NUD) is performed. A shorter duration indicates that the device detects unreachable neighbors more quickly but more network bandwidth and device resources will be consumed. Therefore, you are not advised to set the duration to a very small value.

This command can be configured on an interface or in global configuration mode. The configuration configured on an interface takes priority over that configured in global configuration mode. That is, if the duration is configured on an interface, the duration configured on the interface applies. Otherwise, the global configuration will apply.

Examples

The following example sets the duration in which a neighbor keeps in stale state to 600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd stale-time 600
```

The following example sets the duration in which a neighbor keeps in stale state to 600s on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# ipv6 nd stale-time 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 ipv6 nd suppress-auth-vlan-ns

Function

Run the **ipv6 nd suppress-auth-vlan-ns** command to configure an interface not to send NS packets to an authenticated VLAN.

Run the **no** form of this command to remove this configuration.

Interfaces in an IPv6-enabled super VLAN will not send NS packets to an authenticated sub VLANs by default.

Syntax

ipv6 nd suppress-auth-vlan-ns

no ipv6 nd suppress-auth-vlan-ns

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The command is supported only on SVIs and takes effect in gateway authentication mode.

Examples

The following example configures SVI 2 to send NS packets to an authenticated VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 2
Hostname(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 ipv6 nd suppress-ra

Function

Run the **ipv6 nd suppress-ra** command to configure an interface not to send RA packets.

Run the **no** form of this command to remove this configuration.

IPv6 interfaces do not send RA packets by default.

Syntax

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures port GigabitEthernet 0/1 not to send RA packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd suppress-ra
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.38 ipv6 nd unresolved

Function

Run the **ipv6 nd unresolved** command to configure the maximum number of unresolved ND entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of unresolved ND entries is 0 by default, indicating no restriction. That is, the number of unresolved ND entries is subject to the ND entry capacity supported by the device.

Syntax

ipv6 nd unresolved *number*

no ipv6 nd unresolved

Parameter Description

number: Maximum number of unresolved ND entries. The value range is from 1 to 8000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent malicious scanning attacks from causing the generation of a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Examples

The following example sets the maximum number of unresolved ND entries to 200.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd unresolved 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 ipv6 neighbor

Function

Run the **ipv6 neighbor** command to configure a static neighbor entry.

Run the **no** form of this command to remove this configuration.

No static neighbor entry is configured by default.

Syntax

ipv6 neighbor *ipv6-address interface-type interface-number mac-address*

no ipv6 neighbor *ipv6-address interface-type interface-number*

Parameter Description

ipv6-address: IPv6 address of a neighbor, which must comply with the address representation format in RFC 4291.

interface-type interface-number: Type and number of the interface to which the neighbor resides.

mac-address: Link address of a neighbor, that is, 48-bit MAC address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is similar to the **arp** command. A static neighbor entry can be configured on IPv6-enabled interfaces only. If the neighbor entry to be configured has been learned through NDP and stored in the neighbor table, the dynamic neighbor entry will be automatically converted into a static one. An effective static neighbor entry will be always reachable.

An invalid static neighbor entry refers to a static neighbor entry with the configured IPv6 address not matching the address configured on the interface (not within any IPv6 network segment of this interface, or in conflict with the address of this interface). In this case, packets will not be forwarded through the MAC address specified in the static neighbor entry. An invalid static neighbor entry is inactive. You can run the **show ipv6 neighbor static** to display the validity status of this static neighbor entry.

Examples

The following example configures a static neighbor entry on VLAN 1, with the IP address of 2001::1 and MAC address of 00d0.f811.1111.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **clear ipv6 neighbors**
- **show ipv6 neighbors**

1.40 ipv6 ns-linklocal-src

Function

Run the **ipv6 ns-linklocal-src** command to configure the link-local address as the source address for sending NS packets.

Run the **no** form of this command to remove this configuration.

The link-local address is always used as the source address for sending NS packets by default.

Syntax

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **no ipv6 ns-linklocal-src** command is used to cancel configuring the link-local address as the source address for sending NS packets. Instead, a link-local address or global unicast address is used based on the destination IPv6 address according to RFC 3484.

Examples

The following example configures not to use the link-local address as the source address for sending NS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ipv6 ns-linklocal-src
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

-

1.41 ipv6 redirects

Function

Run the **ipv6 redirects** command to enable the ICMPv6 redirection function.

Run the **no** form of this command to disable this feature.

The ICMPv6 redirection function is enabled by default.

Syntax

ipv6 redirects

no ipv6 redirects

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the ICMPv6 redirection function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 interface**

1.42 ipv6 source-route

Function

Run the **ipv6 source-route** command to configure the device to forward IPv6 packets carrying the routing header.

Run the **no** command to forbid the device from forwarding IPv6 packets carrying the routing header.

IPv6 packets carrying the routing header are not forwarded by default.

Syntax

ipv6 source-route

no ipv6 source-route

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Since the Type 0 routing header may cause the device vulnerable to DoS attacks, the device is forbidden from forwarding IPv6 packets carrying the routing header by default. However, the device still processes IPv6 packets that carry the Type 0 routing header and are finally destined for the device itself.

Examples

The following example configures the device to forward IPv6 packets carrying the routing header.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source-route
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 local-proxy-nd enable

Function

Run the **local-proxy-nd enable** command to enable the local ND proxy function on an interface.

Run the **no** form of this command to disable this feature

Local ND proxy is disabled on an interface by default.

Syntax

local-proxy-nd enable [**force**]

no local-proxy-nd enable

Parameter Description

force: Forcibly enables local ND proxy. That is, an interface always serves as a proxy to respond to NS packets regardless of whether the destination device exists.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If L2 access isolation or inter-subnet isolation (such as sub VLANs) is configured, after local ND proxy is enabled on the gateway, the gateway serves as a proxy to process NS packets from downlink users and replies with NA packets containing the gateway's MAC address. Thus, the traffic of communication among these users is forwarded by the gateway atL3.

Examples

The following example enables local ND proxy on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# local-proxy-nd enable
```

The following example enables forcible local ND proxy on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface VLAN 1
Hostname(config-if-VLAN 1)# local-proxy-nd enable force
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show ipv6 address

Function

Run the **show ipv6 address** command to display the information about an IPv6 address.

Syntax

show ipv6 address [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. All IPv6 addresses are displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all configured IPv6 addresses.

```
Hostname> enable
Hostname# show ipv6 addr
Global unicast address limit: 1024, Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
 GigabitEthernet 0/5
   2003:1::23/64                        Tentative
 Preferred lifetime: INFINITE, Valid lifetime: INFINITE
   fe80::2d0:f8ff:fefb:deb2/64               Tentative
 Preferred lifetime: INFINITE, Valid lifetime: INFINITE
   2005:1::1111/64                       Tentative
```

```
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

The following example displays the IPv6 address configured on port GigabitEthernet 0/1.

```
 Hostname> enable
Hostname# show ipv6 addr gi 0/1
Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
   2003:1::23/64                         Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
   fe80::2d0:f8ff:fefb:deb2/64                Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
   2005:1::1111/64                        Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

Table 1-1 Output Fields of the show ipv6 address Command

Field	Description
Global unicast address count	Number of global unicast IPv6 address configured on this interface.
Tentative address count	Number of tentative addresses.
Duplicate address count	Number of duplicate addresses.
Preferred address count	Number of preferred addresses.
Deprecated address count	Number of expired addresses.
Preferred lifetime	Preferred lifetime.
Valid lifetime	Valid lifetime.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show ipv6 general-prefix

Function

Run the **show ipv6 general-prefix** command to display the prefix information in a general prefix.

Syntax

show ipv6 general-prefix

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

After this command is ran, general prefixes that are manually configured and learned by the DHCPV6 client are displayed.

Examples

The following example displays the prefix information in a general prefix.

```
Hostname> enable
Hostname# show ipv6 general-prefix
There is 1 general prefix.
Ipv6 general prefix my-prefix, acquired via Manual configuration
       2001:1111:2222::/48
       2001:1111:3333::/48
```

Table 1-2 Output Fields of the show ipv6 general-prefix Command

Field	Description
There is	Number of current general prefixes.
IPv6 general prefix	Name of a general prefix.
acquired via	Prefix acquisition method.
Prefix/len	Prefix list.

Notifications

N/A

Platform Description

N/A

1.46 show ipv6 interface

Function

Run the **show ipv6 interface** command to display the information about an IPv6 interface.

Syntax

show ipv6 interface [[*interface-type interface-number*] [**ra-info**] | **brief** [*interface-type interface-number*]]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the information about all IPv6 interfaces is displayed.

ra-info: Displays the parameter information of RA packets on this interface.

brief: Displays the brief information of an interface, including status and address information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command can be used to display address configuration, ND configuration, and statistics of an IPV6 interface.

Examples

The following example displays the information about an IPv6 interface.

```
Hostname> enable
Hostname# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

The command output displays the following line: INET6: 2001::1, subnet is 2001::/64 [TENTATIVE]. The flag bits in [ ] after the IPv6 address are defined as follows.

Table 1-3 Output Fields of the show ipv6 interface vlan 1 Command

Field	Description
ANYCAST	Anycast address.
TENTATIVE	DAD is being performed on the address. This address is tentative before the detection ends.
DUPLICATED	A duplicate address has been detected for this address.
DEPRECATED	This address reaches the preferred lifetime, and the address becomes deprecated.
NODAD	No DAD will be performed on this address.
AUTOIFID	The interface identifier for this address is automatically generated by the system, usually, an EUI-64 identifier.
PRE	Automatically configured stateless address.
GEN	Address generated by general prefix.

The following example displays the parameter information of RA packets on the IPv6 interface.

```
Hostname> enable
Hostname# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime:2592000,pltime:604800, flags: LA)
```

Table 1-4 Output Fields of the show ipv6 interface vlan 1 ra-info Command

Field	Description
RA timer is stopped (on)	Whether the RA packet sending timer is started.
waits	Number of RS packets that have been received but not responded to.
initcount	Number of RA packets initially sent when the RA timer restarts.

Field	Description
RA (out/in/inconsistent)	RA packets. ● **Out**: Indicates the number of RA packets sent. ● **In**: Indicates the number of RA packets received. ● **Inconsistent**: Indicates the number of received RA packets with parameters inconsistent with those advertised by the router itself.
RS (input)	Number of RS packets received.
Link-layer address	Link layer address of this interface.
Physical MTU	Link MTU of this interface.
!M | M	● **!M** indicates that the **Managed-config-flag** option is not carried in an RA packet. ● **M** indicates that the **Managed-config-flag** option is carried in an RA packet.
!O | O	● **!O** indicates that the **Other-config-flag** option is not carried in an RA packet. ● **O** indicates that the **Other-config-flag** option is carried in an RA packet.
total	Number of prefixes on this interface.
fec0:1:1:1::/64	Specific prefix.
Def	Default prefix configuration is used for this prefix.
Auto | CFG	● **Auto** indicates that this prefix is automatically generated since the corresponding IPv6 address is configured on an interface. ● **CFG** indicates that this prefix is manually configured.
!Adv	This prefix will not be advertised.
vltime	Valid lifetime of this prefix, in seconds.
pltime	Preferred lifetime of this prefix, in seconds.
L | !L	● **L** indicates that the prefix is On-link. ● **!L** indicates that the prefix is Off-link.
A | !A	● **A** indicates that the prefix can be automatically configured. ● **!A** indicates that the prefix cannot be automatically configured.

The following example displays the brief information of an IPv6 interface.

```
Hostname> enable
Hostname# show ipv6 interface brief
```

```
GigabitEthernet 0/1         [down/down]
       2222::2
       FE80::1614:4BFF:FE5C:ED3A
```

Table 1-5 Output Fields of the show ipv6 interface brief Command

Field	Description
GigabitEthernet 0/1	Interface name.
down/down	Link status or IPv6 protocol status of an interface.
2222::2	Primary IPv6 address of an interface.
FE80::1614:4BFF:FE5C:ED3A	Secondary IPv6 address of an interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 show ipv6 nd

Function

Run the **show ipv6 nd** command to display the statistics on IPv6 ND packets.

Syntax

show ipv6 nd [**interface** *interface-type interface-number*] **statistics**

Parameter Description

interface *interface-type interface-number*: Specifies the type and number of an IPv6 interface. After this parameter is configured, ND packet statistics of this interface will be displayed.

statistics: Displays the statistics on ND packets.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics on IPv6 ND packets of SVI 1.

```
Hostname> enable
Hostname# show ipv6 nd interface vlan 1 statistics
interface VLAN 1 is Up, ifindex: 4097, vrf_id 0
 ipv6 interface packet statics:
 stat-type             Router Solicitations           Router advertisements
Neighbor solicitations         Neighbor advertisements
 Received              0                            0                             0
0
 Send                 0                            0                             1
0
 Rate(receive, pps)      0                            0                             0
0
 Rate(send, pps)         0                            0                             0
0
 Interval time: 60s
```

Table 1-6 Output Fields of the show ipv6 nd Command

Field	Description
stat-type	Statistics type: RS/RA/NS/NA packets.
Received	Statistics on received packets.
Send	Statistics on sent packets.
Rate	Packet transmission/receiving rate, in PPS.
Interval time	Sampling interval of ND packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 show ipv6 neighbors

Function

Run the **show ipv6 neighbors** command to display IPv6 neighbor tables.

Syntax

show ipv6 neighbors [**vrf** *vrf-name*] [**verbose**] [*interface-type interface-number*] [*ipv6-address*] [**static**] [**oob**]

Parameter Description

vrf *vrf-name*: Specifies a VRF instance.

verbose: Displays detailed neighbor information.

interface-type interface-number: Interface type and interface number. After this parameter is configured, the neighbor table of an interface will be displayed. The neighbor tables of all interfaces are displayed by default.

ipv6-address: IPv6 address. After this parameter is configured, information about a specified neighbor will be displayed.

static: Displays the status of a static neighbor entry.

oob: Displays the IPv6 neighbors of the management interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the neighbor table on SVI 1.

```
Hostname> enable
Hostname# show ipv6 neighbors vlan 1
Ipv6 Address Linklayer Addr   Interface
fa::1        00d0.0000.0002   vlan 1
fe80::200:ff:fe00:2  00d0.0000.0002  vlan 1
```

The following example displays details about a neighbor

```
Hostname> enable
Hostname# show ipv6 neighbors verbose
Ipv6 Address  Linklayer Addr Interface
2001::1      00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1    00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
```

Table 1-7 Output Fields of the show ipv6 neighbors Command

Field	Description
IPv6 Address	IPv6 address of a neighbor.

Field	Description
Linklayer Addr	Link address, that is, MAC address. If this address is not obtained, "incomplete" is displayed.
Interface	Interface where the neighbor resides.
State	Status of the neighbor. ● **INCMP** (Incomplete) indicates that the address resolution of the neighbor is underway, the NS packet has been sent, but no reply packet is received from the neighbor. ● **REACH** (Reachable) indicates that the device is reachable to the neighbor and no additional action is required to send packets to the neighbor. ● **STALE** indicates that the time that the neighbor considered reachable has elapsed. In this state, no additional action is required on the device until a packet is sent to the neighbor. Then, the device performs NUD. ● **DELAY** indicates that a packet is sent to the neighbor in stale state. The neighbor changes from STALE state to DELAY state. If no notification indicating that the neighbor is reachable is received within DELAY_FIRST_PROBE_TIME seconds (5 seconds), then the neighbor will change from DELAY state to PROBE state, and an NS packet will be sent to the neighbor to officially start NUD. ● **PROBE** indicates that NUD has been started to detect the neighbor reachability. NS packets are sent to the neighbor every RetransTimer milliseconds until reply packets are received or the number of NS packets sent reaches the limit MAX_UNICAST_SOLICIT (three NS packets). ● **?** indicates unknown state. ● **/R** indicates that the neighbor is deemed as a device. ● **/H** indicates that the neighbor is deemed as a host.
Age	Amount of time that a neighbor is considered reachable. ● **-** indicates that a neighbor is always reachable. Static neighbor entries will rely on whether they are actually reachable. ● **expired** indicates the amount of time that a neighbor is considered reachable has elapsed and NUD is to be triggered.
Asked	Number of NS packets sent to a neighbor during the resolution of the neighbor's link address.

The following example displays the status of static neighbor entries.

```
Hostname> enable
Hostname# show ipv6 neighbors static
Ipv6 Address    Linklayer Addr  Interface              State
2001:1::1       00d0.f822.33ab  GigabitEthernet 0/14   ACTIVE
2001:2::2       00d0.f822.33ac  VLAN 1                 INACTIVE
```

Table 1-8 Output Fields of the show ipv6 neighbors static Command

Field	Description
IPv6 Address	IPv6 address of a static neighbor entry.
Linklayer Addr	Link address, that is, MAC address.
Interface	Interface where the neighbor resides.
State	Status of a static neighbor entry. The value of **State** includes: ● **ACTIVE**, indicating that a static neighbor entry is active. ● **INACTIVE**, indicating that a static neighbor entry is inactive. When the IPv6 address configured for a static neighbor entry does not match that on the interface (not within any address segment of this interface, or in conflict with the address of this interface), the static neighbor entry is inactive, that is, packets will not be forwarded through the MAC address specified in the static neighbor entry.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 show ipv6 neighbors statistics

Function

Run the **show ipv6 neighbors statistics** command to display the statistics on IPv6 neighbor tables.

Syntax

show ipv6 neighbors [**vrf** *vrf-name*] **statistics** [**all**]

Parameter Description

vrf *vrf-name*: Specifies the name of a VRF instance.

all: Displays the statistics on all IPv6 neighbor tables.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics on global IPv6 neighbor tables.

```
Hostname> enable
Hostname# show ipv6 neighbor statistics
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
```

The following example displays the statistics on all IPv6 neighbor tables.

```
Hostname> enable
Hostname# show ipv6 neighbor statistics all
Ipv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
```

Table 1-9 Output Fields of the show ipv6 neighbors statistics Command

Field	Description
IPv6 neighbor table count	Number of neighbor tables
Static neighbor count	Number of static neighbor entries.
active	Number of active neighbor entries.
inactive	Number of inactive neighbor entries.
Memory	Memory usage.
Entries	Number of neighbor entries.
Static	Number of static entries.
Dynamic	Number of dynamic entries.
Local	Number of entries corresponding to the local IPv6 address.
Incomplete	Number of unresolved entries.

Field	Description
Reachable	Number of reachable neighbor entries.
Stale	Number of entries in stale state.
Delay	Number of entries in the delay state.
Probe	Number of entries in the probe state.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.50 show ipv6 packet statistics

Function

Run the **show ipv6 packet statistics** command to display the statistics on IPv6 packets.

Syntax

show ipv6 packet statistics [**total** | *interface-type interface-number*]

Parameter Description

total: Specifies the sum of the statistics on all interfaces. If this parameter is not specified, the sum of the statistics of all interfaces as well as the statistics of each interface are displayed.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the sum of the statistics on IPv6 packets and the statistics of each interface.

```
Hostname> enable
Hostname# show ipv6 pack statistics
Total
```

```
 Received 0 packets, 0 bytes
   Unicast:0,Multicast:0
   Discards:0
     HdrErrors:0(HoplimitExceeded:0,Others:0)
     NoRoutes:0
     Others:0
 Sent 0 packets, 0 bytes
   Unicast:0,Multicast:0
 GigabitEthernet 0/5
 Received 0 packets, 0 bytes
   Unicast:0,Multicast:0
   Discards:0
     HdrErrors:0(HoplimitExceeded:0,Others:0)
     NoRoutes:0
     Others:0
 Sent 0 packets, 0 bytes
   Unicast:0,Multicast:0
```

The following example displays the sum of the statistics on IPv6 packets.

```
Hostname> enable
Hostname# show ipv6 pack statistics total
Total
 Received 0 packets, 0 bytes
   Unicast:0,Multicast:0
   Discards:0
     HdrErrors:0(HoplimitExceeded:0,Others:0)
     NoRoutes:0
     Others:0
 Sent 0 packets, 0 bytes
   Unicast:0,Multicast:0
```

Table 1-10 Output Fields of the show ipv6 pack statistics Command

Field	Description
Total	Sum of the statistics on IPv6 packets of all interfaces.
Received	Number of received IPv6 packets, in bytes.
Unicast	Number of IPv6 unicast packets.
Multicast	Number of IPv6 multicast packets.
Discards	Number of discarded IPv6 packets.
HdrErrors	Number of IPv6 packets discarded due to header error.
HoplimitExceeded	Number of packets discarded due to hop limit overrange during forwarding.
Others	Number of other IPv6 packets discarded due to header error.

Field	Description
NoRoutes	Number of IPv6 packets discarded due to no routing.
Others	Number of IPv6 packets discarded due to other reasons.
Sent	Number of sent IPv6 packets, in bytes.
Unicast	Number of unicast packets.
Multicast	Number of multicast packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 show ipv6 raw-socket

Function

Run the **show ipv6 raw-socket** command to displays all IPv6 raw sockets.

Syntax

show ipv6 raw-socket [*protocol*]

Parameter Description

protocol: Protocol number. The value range is from 1 to 255.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all IPv6 raw sockets.

```
Hostname> enable
Hostname# show ipv6 raw-socket
Number Protocol Process name
1     ICMPv6   vrrp.elf
```

```
2     ICMPv6   tcpip.elf
3     VRRP     vrrp.elf
Total: 3
```

Table 1-11 Output Fields of the show ipv6 raw-socket Command

Field	Description
Number	Serial number.
Protocol	Protocol number.
Process name	Process name.
Total	Total number of IPv6 raw sockets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 show ipv6 routers

Function

Run the **show ipv6 routers** command to display neighbor router information and RA packets.

Syntax

show ipv6 routers [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. After this parameter is specified, RA packets received by a specified interface will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no interface is specified, then the information about RA packets received by this device is displayed.

Examples

The following example displays neighbor router information and RA packets.

```
Hostname> enable
Hostname# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
  Preference=MEDIUM
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 6001:3::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800 sec
  Prefix 6001:2::/64 onlink autoconfig
Valid lifetime 2592000 sec, preferred lifetime 604800 sec
```

Table 1-12 Output Fields of the show ipv6 routers Command

Field	Description
Router	Neighbor router, which is described using the IPv6 address and the network interface receiving RA packets.
last update	Time that has elapsed since the last RA packet is received.
Hops	Hop count of RA packets.
Lifetime	Lifetime of the router.
ManagedFlag	Managed flag of the router.
OtherFlag	Other flag of the router.
MTU	MTU of the interface sending RA packets on the router.
Reachable time	Amount of time that the router is considered reachable.
Retransmit time	RA packet retransmission time of the router.
Prefix	Prefix of RA packets.
Valid lifetime	Lifetime of a prefix.
preferred lifetime	Preferred lifetime of a prefix.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.53 show ipv6 sockets

Function

Run the **show ipv6 sockets** command to display all IPv6 raw sockets.

Syntax

show ipv6 sockets

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display all IPv6 sockets and thus obtain the UDP port and TCP port that provide services for external devices.

Examples

The following example displays all IPv6 sockets.

```
Hostname> enable
Hostname# show ipv6 sockets
Number Process name    Type   Protocol  LocalIP:Port  ForeignIP:Port  State
1     vrrp.elf        RAW    ICMPv6    :::58         :::0            *
2     tcpip.elf       RAW    ICMPv6    :::58         :::0            *
3     vrrp.elf        RAW    VRRP     :::112         :::0            *
4     rg-snmpd        DGRAM  UDP      :::161         :::0            *
5     rg-snmpd        DGRAM  UDP      :::162         :::0            *
6     dhcp6.elf       DGRAM  UDP      :::547         :::0            *
7     rg-sshd         STREAM TCP      :::22          :::0           LISTEN
8     rg-telnetd      STREAM TCP       :::23          :::0           LISTEN
Total: 8
```

Table 1-13 Output Fields of the show ipv6 sockets Command

Field	Description
Number	Serial number.
Process name	Process name.

Field	Description
Type	Socket type. ● **RAW** indicates a raw socket. ● **DGRAM** indicates the packet type. ● **STREAM** indicates the stream type.
Protocol	Protocol number.
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	Status (only for IPv6 TCP sockets).
Total	Total number of sockets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.54 show ipv6 udp

Function

Run the **show ipv6 udp** command to display all IPv6 UDP sockets.

Syntax

show ipv6 udp [**local-port** *port-number*] [**peer-port** *port-number*]

Parameter Description

local-port *port-number*: Specifies a local port number.

peer-port *port-number*: Specifies a peer port number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display all IPv6 UDP sockets and thus learn the UDP port that provides services for external devices.

Examples

The following example displays all IPv6 UDP sockets.

```
Hostname> enable
Hostname# show ipv6 udp
Number Local Address   Peer Address   Process name
1      :::161          :::0         rg-snmpd
2      :::162          :::0         rg-snmpd
3      :::547          :::0         dhcp6.elf
```

Table 1-14 Output Fields of the show ipv6 udp Command

Field	Description
Number	Serial number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.55 show ipv6 udp statistics

Function

Run the **show ipv6 udp statistics** command to display the statistics on IPv6 UDP sockets.

Syntax

show ipv6 udp statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics on all IPv6 UDP sockets.

```
Hostname> enable
Hostname# show ipv6 udp statistics
Number of Ipv6 UDP sockets is 3.
```

Figure 1-1 Output Fields of the show ipv6 udp Command

Field	Description
Number of Ipv6 UDP sockets is x	The total number of IPv6 UDP sockets is x.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 DHCPv6 Commands

Command	Function
bootfile-url	Configure the boot file Uniform Resource Locator (URL) that a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server assigns to a DHCPv6 client.
clear ipv6 dhcp binding	Clear bindings on a DHCPv6 server.
clear ipv6 dhcp conflict	Clear conflicted addresses on a DHCPv6 server.
clear ipv6 dhcp relay statistics	Clear statistics of different types of packets on a DHCPv6 relay agent.
clear ipv6 dhcp server statistics	Clear statistics of different types of packets on a DHCPv6 server.
dns-server	Configure the Domain Name System (DNS) server address to be assigned from a DHCPv6 server to a DHCPv6 client.
domain-name	Configure the domain name to be assigned from a DHCPv6 server to a DHCPv6 client.
excluded-address	Configure excluded network segments on a DHCPv6 server.
iana-address prefix	Configure the IA_NA address prefix to be assigned from a DHCPv6 server to a DHCPv6 client.
ipv6 dhcp pool	Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.
ipv6 dhcp relay destination	Enable the DHCPv6 Relay function and specify a destination address.
ipv6 dhcp relay option interface-id format user-defined	Configure the Interface ID option on a DHCPv6 relay agent.
ipv6 dhcp relay option mac-str-format	Configure the format of the MAC address in the user-defined Option on a DHCPv6 relay agent.
ipv6 dhcp relay option remote-id enable	Add the Remote ID option to DHCPv6 relay packets.
ipv6 dhcp relay option remote-id format user-defined	Configure the value of Remote ID in DHCPv6 relay packets.

ipv6 dhcp relay source	Configure the source interface of a DHCPv6 relay agent.
ipv6 dhcp server	Enable the DHCPv6 Server function on an interface.
ipv6 local pool	Configure a local prefix pool for the PD service of a DHCPv6 server.
option52	Configure the IPv6 address of a Control and Provisioning of Wireless Access Points (CAPWAP) access controller (AC) specified on a DHCPv6 server.
prefix-delegation	Configure prefixes for statically bound addresses on a DHCPv6 server.
prefix-delegation pool	Configure a local prefix pool on a DHCPv6 server.
show ipv6 dhcp	Display the DUID of a DHCPv6 device.
show ipv6 dhcp binding	Display address bindings on a DHCPv6 server.
show ipv6 dhcp conflict	Display conflicted addresses on a DHCPv6 server.
show ipv6 dhcp interface	Display DHCPv6 interfaces.
show ipv6 dhcp pool	Display DHCPv6 address pools.
show ipv6 dhcp relay agent	Display source interfaces on a DHCPv6 relay agent.
show ipv6 dhcp relay destination	Display destination addresses on a DHCPv6 relay agent.
show ipv6 dhcp relay source	Display the source interface definition configuration on a DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Display statistics of different types of packets on a DHCPv6 relay agent.
show ipv6 dhcp server statistics	Displays DHCPv6 server statistics.
show ipv6 local pool	Display local prefix pool configuration and usage on the current device.

1.1 bootfile-url

Function

Run the **bootfile-url** command to configure the boot file Uniform Resource Locator (URL) that a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server assigns to a DHCPv6 client.

Run the **no** form of this command to remove this configuration.

No boot file URL is configured by default.

Syntax

bootfile-url *url-string*

no bootfile-url

Parameter Description

url-string: Boot file URL. The value is a case-sensitive string of 1 to 256 characters.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

When this command is run on a DHCPv6 address pool multiple times, the last configuration prevails.

Examples

The following example sets the boot file URL in DHCPv6 address pool pool1 to tftp://1000::1/boot.bin.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# bootfile-url tftp://1000::1/boot.py
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.2 clear ipv6 dhcp binding

Function

Run the **clear ipv6 dhcp binding** command to clear bindings on a DHCPv6 server.

Syntax

clear ipv6 dhcp binding [*ipv6-address*]

Parameter Description

ipv6-address: IPv6 address or prefix.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the *ipv6-address* parameter is not configured, all bindings on a DHCPv6 server are cleared. If the *ipv6-address* parameter is configured, only bindings of the specified address or prefix are cleared.

Examples

The following example clears all bindings on a DHCPv6 server.

```
Hostname> enable
Hostname# clear ipv6 dhcp binding
```

Notifications

When binding information of the specified address or prefix cannot be found, the following notification will be displayed:

```
Failed to clear DHCPv6 binding x:x:x:x:x:x:x:x, please try again
```

Platform Description

N/A

1.3 clear ipv6 dhcp conflict

Function

Run the **clear ipv6 dhcp conflict** command to clear conflicted addresses on a DHCPv6 server.

Syntax

clear ipv6 dhcp conflict { *ipv6-address* | * }

Parameter Description

ipv6-address: IPv6 address or prefix.

*: All IPv6 addresses or prefixes.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

To clear all conflicted addresses when the *ipv6-address* parameter is not configured, add an asterisk (*) after this command, which represents all IPv6 addresses or prefixes. If the *ipv6-address* parameter is configured, only conflict information of the specified address is cleared.

When a DHCPv6 client detects that the assigned IPv6 address is in conflict, it sends a DECLINE packet to the DHCPv6 server. The DHCPv6 server adds the address to the address conflict queue.

Examples

The following example clears conflicted addresses on a DHCPv6 server.

```
Hostname> enable
Hostname# clear ipv6 dhcp conflict 2008:50::2
```

Notifications

N/A

Platform Description

N/A

1.4 clear ipv6 dhcp relay statistics

Function

Run the **clear ipv6 dhcp relay statistics** command to clear statistics of different types of packets on a DHCPv6 relay agent.

Syntax

clear ipv6 dhcp relay statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics of different types of packets on a DHCPv6 relay agent.

```
Hostname> enable
Hostname# clear ipv6 dhcp relay statistics
```

Notifications

N/A

Platform Description

N/A

1.5 clear ipv6 dhcp server statistics

Function

Run the **clear ipv6 dhcp server statistics** command to clear statistics of different types of packets on a DHCPv6 server.

Syntax

clear ipv6 dhcp server statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics of different types of packets on a DHCPv6 server.

```
Hostname> enable
Hostname# clear ipv6 dhcp server statistics
```

Notifications

N/A

Platform Description

N/A

1.6 dns-server

Function

Run the **dns-server** command to configure the Domain Name System (DNS) server address to be assigned from a DHCPv6 server to a DHCPv6 client.

Run the **no** form of this command to remove this configuration.

No DNS server address is configured by default.

Syntax

dns-server *ipv6-address*

no dns-server *ipv6-address*

Parameter Description

ipv6-address: DNS server address to be assigned to a DHCPv6 client.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

You can run this command multiple times to create multiple DNS server addresses. New DNS server addresses do not overwrite old one. A maximum of 10 DNS server addresses can be configured.

Examples

The following example sets the DNS server address in DHCPv6 address pool pool1 to **2008:1::1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# dns-server 2008:1::1
```

Notifications

When the number of configured DNS server addresses exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 dns limit for each pool, 10.
```

When the configured DNS server address is incorrect, the following notification will be displayed:

```
Configure dhcpv6 dns-server with an invalid unicast ipv6 address.
```

When the DNS server address configuration fails, the following notification will be displayed:

```
Failed to configure DNS address, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.7 domain-name

Function

Run the **domain-name** command to configure the domain name to be assigned from a DHCPv6 server to a DHCPv6 client.

Run the **no** form of this command to remove this configuration.

No domain name is configured by default.

Syntax

domain-name *domain*

no domain-name *domain*

Parameter Description

domain: Domain name to be assigned to a DHCPv6 client. The value is a case-sensitive string of 1 to 255 characters.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

You can run this command multiple times to create multiple domain names. New domain names do not overwrite old ones. A maximum of 10 domain names can be configured.

Examples

The following example sets the domain name in DHCPv6 address pool pool1 to **example.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# domain-name example.com
```

Notifications

When the number of configured domain names exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 domain name limit for each pool, 10.
```

When domain name configuration fails, the following notification will be displayed:

```
Failed to configure domain name, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.8 excluded-address

Function

Run the **excluded-address** command to configure excluded network segments on a DHCPv6 server.

Run the **no** form of this command to remove this configuration.

After an address pool is created, no excluded network segment is configured on a DHCPv6 server by default.

Syntax

excluded-address *start-ipv6-address* [*end-ipv6-address*]

no excluded-address *start-ipv6-address* [*end-ipv6-address*]

Parameter Description

start-ipv6-address: Start IPv6 address in an excluded network segment.

end-ipv6-address: End IPv6 address in an excluded network segment. If this parameter is not configured or is the same as the start IPv6 address, a single IPv6 address is excluded.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

You can run this command multiple times to create multiple excluded network segments.

Before creating an excluded network segment, you need to configure the corresponding identity association non-temporary address (IA_NA) network segment, and the excluded network segment must belong to the IA_NA network segment. After an IA_NA network segment is deleted, excluded network segments belonging to this segment are deleted automatically. After an excluded network segment is created, online entries of users in this network segment are deleted automatically.

Examples

The following example excludes addresses in the network segment from 1000::100 to 1000::200 in DHCPv6 address pool pool1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 dhcp pool pool1
Hostname(dhcp-config)# excluded-address 1000::100 1000::200
```

Notifications

When the number of configured excluded network segments exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 exclude address limit for each pool, 1000.
```

When a configured excluded network segment does not belong to any IA_NA network segment, the following notification will be displayed:

```
Configure dhcpv6 iana address first before the exclude range.
```

When a configured excluded network segment conflicts with another excluded network segment, the following notification will be displayed:

```
Configure dhcpv6 exclude conflict with other exclude range.
```

When an excluded network segment fails to be configured, the following notification will be displayed:

```
Failed to configure exclude address, please try again.
```

Common Errors

No IA_NA network segment is configured before excluded addresses are configured.

Platform Description

N/A

Related Commands

N/A

1.9 iana-address prefix

Function

Run the **iana-address prefix** command to configure the IA_NA address prefix to be assigned from a DHCPv6 server to a DHCPv6 client.

Run the **no** form of this command to remove this configuration.

No IA_NA address prefix is configured by default.

Syntax

iana-address prefix *ipv6-address/prefix-length* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** } }]

no iana-address prefix

Parameter Description

ipv6-address/prefix-length: IPv6 address or prefix length.

lifetime: Specifies the valid time of an address to be assigned to a DHCPv6 client.

valid-lifetime: Valid time for a DHCPv6 client to use an assigned address, in seconds. The range is from 60 to 4294967295. The default value is **3600**.

preferred-lifetime: Time during which an address is still preferentially assigned to a client, in seconds. The range is from 60 to 4294967295. The default value is **3600**.

infinite: Indicates that an IA_NA address prefix is permanently valid.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

After an IA_NA address prefix is configured by running this command, a DHCPv6 server can assign an IA_NA address with this prefix to a DHCPv6 client.

When receiving an IA_NA address request from a DHCPv6 client, the DHCPv6 server selects an available address based on the IA_NA address prefix and assigns the address to the client. When the client no longer needs this address, the DHCPv6 server marks this address as available for other clients.

Examples

The following example configures an IA_NA address prefix 2008:50::/64 in DHCPv6 address pool pool1, sets the valid time for a client to use an assigned address with this prefix to 2000s, and sets the time during which the address is still preferentially assigned to the client to 1000s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#ipv6 dhcp pool pool1
Hostname(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000
```

Notifications

When the value of *valid-lifetime* is smaller than that of *preferred-lifetime*, the following notification will be displayed:

```
Preferred lifetime must not exceed valid lifetime.
```

When the number of configured address prefixes exceeds the limit, the following notification will be displayed:

```
iana range number has reached the max 20.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.10 ipv6 dhcp pool

Function

Run the **ipv6 dhcp pool** command to create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

Run the **no** form of this command to remove this configuration.

No DHCPv6 address pool is configured by default.

Syntax

ipv6 dhcp pool *pool-name*

no ipv6 dhcp pool *pool-name*

Parameter Description

pool-name: DHCPv6 address pool name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to create a DHCPv6 address pool. After configuring this command, you can enter the DHCPv6 address pool configuration mode, so as to configure address pool parameters such as the prefix and DNS server address.

After a DHCPv6 address pool is created, you can run the **ipv6 dhcp server** command on an interface to associate the address pool with the DHCPv6 server on the interface.

Examples

The following example creates a DHCPv6 address pool named **pool1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)#
```

Notifications

When the number of configured address pools exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 pool limit 256.
```

When address pool configuration fails, the following notification will be displayed:

```
Failed to configure dhcpv6 pool xxx, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.11 ipv6 dhcp relay destination

Function

Run the **ipv6 dhcp relay destination** command to enable the DHCPv6 Relay function and specify a destination address.

Run the **no** form of this command to disable this feature.

The DHCPv6 Relay function is disabled by default.

Syntax

ipv6 dhcp relay destination [**vrf** *vrf-name*] *ipv6-address* [*interface-type interface-number*]

no ipv6 dhcp relay destination [**vrf** *vrf-name*] *ipv6-address* [*interface-type interface-number*]

Parameter Description

vrf *vrf-name*: Specifies a virtual routing and forwarding (VRF) instance.

ipv6-address: Destination address on a DHCPv6 relay agent.

interface-type interface-number: Type and number of the interface over which packets are routed to the destination address. When the destination address is a multicast address, this parameter is mandatory.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command can be configured only on layer 3 (L3) interfaces.

The total number of destination addresses is 20 at most on all interfaces configured with the DHCPv6 Relay function.

After this function is configured on an interface, all packets received from DHCPv6 clients on this interface are encapsulated and then forwarded to each configured destination address.

Examples

The following example enables the DHCPv6 Relay service on Switch Virtual Interface (SVI) 1 and sets the destination address to **3001::2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
```

```
Hostname(config-if-VLAN 1)# ipv6 dhcp relay destination 3001::2
```

Notifications

When the configured relay address is a local address, the following notification will be displayed:

```
Cannot relay to this relay agent itself.
```

When the DHCPv6 Relay function is configured on an interface that already works in another mode (DHCPv6 server or client), the following notification will be displayed:

```
Interface is in DHCP xxx mode.
```

When the DHCPv6 Relay function fails to be configured, the following notification will be displayed:

```
Failed to configure DHCPv6 relay, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp relay destination**

1.12 ipv6 dhcp relay option interface-id format user-defined

Function

Run the **ipv6 dhcp relay option interface-id format user-defined** command to configure the **Interface ID** option on a DHCPv6 relay agent.

Run the **no** form of this command to remove this configuration.

The interface name is the value of **Interface ID** on a DHCPv6 relay agent by default.

Syntax

ipv6 dhcp relay option interface-id format user-defined *text*

no ipv6 dhcp relay option interface-id format user-defined

Parameter Description

text: Value of user-defined **Interface ID**. The value is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When customizing the format of an option, you can use keywords described in the following table. The format string behind the keywords can be set to the hexadecimal encapsulation format, ASCII encapsulation format, or hexadecimal and ASCII hybrid encapsulation format.

Table 1-1 User-Defined Option Keywords

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
hostname	Host name	√	×	-	Example: Hostname
devicename	Device model	√	×	-	Example: S5750C-48GT4XS-H
portname	Interface name	√	×	-	Example: GigabitEthernet 0/1
portsname	Interface name abbreviation	√	×	-	Example: Te0/2.5
porttype	Interface type	√	√	1 B	Example: ● When ASCII is used to represent 1, the padding value is **0x31**. ● When hexadecimal is used to represent 1, the padding value is **0x01**.
sysmac	Interface MAC address	√	√	6 B	Example: ● ASCII: 2222.2222.2222 ● Hexadecimal: 0x22 0x22 0x22 0x22 0x22 0x22
slot	Slot ID	√	√	1 B	Example: ● When ASCII is used to represent 0, the padding value is **0x30**. ● When hexadecimal is used to

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					represent 0, he padding value is **0x00**.
port	Port number	√	√	1 B	Example: ● When ASCII is used to represent 2, the padding value is **0x32**. ● When hexadecimal is used to represent 2, the padding value is **0x02**.
svlan	Outer VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
cvlan	Inner VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					0x0005.
length	Length of content following the length keyword	×	√	1 B	Example: When hexadecimal is used to represent 5, the padding value is 0x05.

Note: √ indicates that a keyword supports the corresponding encapsulation format, × indicates that a keyword does not support the corresponding encapsulation format, and - indicates meaningless.

Special characters are described as follows:

- % followed by keywords defined above indicates the format of the keywords. When the percent symbol (%) needs to be contained in the input string, enter %%, which will be converted into a single common percent symbol (%) during parsing.
- The backslash (\) indicates an escape character, and the special character following the backslash (\) indicates the special character itself. For example, \\ indicates the backslash (\) and \" indicates the quotation mark (").
- The double quotation marks ("") indicate that data enclosed is encapsulated in string format. Data without or outside the double quotation marks is encapsulated in hexadecimal format.
- Strings in ASCII format can contain 0 to 9, a to z, A to Z, and the following symbols: !, @, #, $, %, ^, &, *, (), _, +, |, -, =, \, [], {}, ;, :, '", /, ?, ., ,, <>, `.
- For characters %\" in ASCII format, add the prefix (\) in front of the characters. In ASCII format, only keywords and several specific symbols are converted and other data remains unchanged.
- If there is no escape character '%' in front of '%' in configuration commands, the key value in the information field must be added behind. Otherwise, the configuration is incorrect and an error is prompted. If the character '\' needs to be configured, enter "\\".
- For strings in hexadecimal format, digits are encapsulated into the option in hexadecimal notation. When hexadecimal data is used, strings begin with 0X or 0x. When the number of valid characters in the hexadecimal data is an odd, add one 0 to the frontmost. When decimal data is used, the data ranges from 0 to 255 and occupies one byte. You can use spaces to enter multiple pieces of decimal data consecutively.
- Blank characters in hexadecimal notation are ignored.

Examples

The following example sets the value of **Interface ID** to the port name and local host MAC address in ASCII format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option interface-id format user-defined
"%portname %sysmac"
```

The following example sets the value of **Interface ID** to the local host MAC address in hexadecimal format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option interface-id format user-defined %sysmac
```

Notifications

When the padding format of a keyword is incorrect (for example, **%portname** can be padded only in ASCII format), the following notification will be displayed:

```
% Format of Keyword unmatched.
```

When a keyword fails to be matched, the following notification will be displayed:

```
% User defined string include bad keyword.
```

When a keyword fails to be identified, the following notification will be displayed:

```
% DHCP6 RELAY could not parse the user defined string.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv6 dhcp relay option mac-str-format

Function

Run the **ipv6 dhcp relay option mac-str-format** command to configure the format of the MAC address in the user-defined Option on a DHCPv6 relay agent.

Run the **no** form of this command to remove this configuration.

The default MAC address format is H.H.H.

Syntax

ipv6 dhcp relay option mac-str-format *type*

no ipv6 **dhcp relay option mac**-**str**-**format**

Parameter Description

type: Format of the MAC address string. The value range is from 1 to 3, and the default value is **1**. **1** indicates the H.H.H format, **2** indicates the H-H-H format, and **3** indicates the H:H:H:H:H:H format.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the format of the MAC address in user-defined options.

Examples

The following example sets the format of the MAC address in user-defined options on a DHCPv6 relay agent to H-H-H.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option mac-str-format 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 dhcp relay option remote-id enable

Function

Run the **ipv6 dhcp relay option remote-id enable** command to add the **Remote ID** option to DHCPv6 relay packets.

Run the **no** form of this command to remove this configuration.

DHCPv6 relay packets do not carry **Remote-ID** by default.

Syntax

ipv6 dhcp relay option remote-id enable

no ipv6 dhcp relay option remote-id enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Remote ID is used to uniquely identify a DHCPv6 client. Based on the value of **Remote ID**, a DHCPv6 server performs address assignment, parameter configuration, and prefix delegation (PD). The value of **Remote ID** is customized by the vendor. Generally, this option carries the DHCP Unique Identifier (DUID) and name of the access device.

Examples

The following example adds **Remote ID** to DHCPv6 relay packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option remote-id enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 dhcp relay option remote-id format user-defined**

1.15 ipv6 dhcp relay option remote-id format user-defined

Function

Run the **ipv6 dhcp relay option remote-id format user-defined** command to configure the value of **Remote ID** in DHCPv6 relay packets.

Run the **no** form of this command to remove this configuration.

The device DUID is specified in **Remote ID** in DHCPv6 relay packets by default.

Syntax

ipv6 dhcp relay option remote-id format user-defined *text*

no ipv6 dhcp relay option remote -id format user-defined

Parameter Description

text: Value of **Remote ID**. The value is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When customizing the format of an option, you can use keywords described in the following table. The format string behind the keywords can be set to the hexadecimal encapsulation format, ASCII encapsulation format, or hexadecimal and ASCII hybrid encapsulation format.

Table 1-2 User-Defined Option Keywords

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
hostname	Host name	√	×	-	Example: Hostname
devicename	Device model	√	×	-	Example: S5750C-48GT4XS-H
portname	Interface name	√	×	-	Example: GigabitEthernet 0/1
portsname	Interface name abbreviation	√	×	-	Example: Te0/2.5
porttype	Interface type	√	√	1 B	Example: ● When ASCII is used to represent 1, the padding value is **0x31**. ● When hexadecimal is used to represent 1, the padding value is **0x01**.
sysmac	Interface MAC address	√	√	6 B	Example: ● ASCII: 2222.2222.2222 ● Hexadecimal: 0x22 0x22 0x22 0x22 0x22 0x22
slot	Slot ID	√	√	1 B	Example: ● When ASCII is used to represent 0, the padding value is **0x30**. ● When hexadecimal is used to represent 0, he padding value is **0x00**.
port	Port number	√	√	1 B	Example: ● When ASCII is used to represent 2, the

Keyword	Name	Format			Description
		ASCII	Hexadecimal	Number of Occupied Hexadecimal Bytes	
					padding value is **0x32**. ● When hexadecimal is used to represent 2, the padding value is **0x02**.
svlan	Outer VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
cvlan	Inner VLAN	√	√	2 B	Example: ● When ASCII is used to represent 5, the padding value is **0x35**. ● When hexadecimal is used to represent 5, the padding value is **0x0005**.
length	Length of content following the length keyword	×	√	1 B	Example: When hexadecimal is used to represent 5, the padding value is **0x05**.

Note: √ indicates that a keyword supports the corresponding encapsulation format, × indicates that a keyword does not support the corresponding encapsulation format, and - indicates meaningless.

Special characters are described as follows:

- % followed by keywords defined above indicates the format of the keywords. When the percent symbol (%) needs to be contained in the input string, enter %%, which will be converted into a single common percent symbol (%) during parsing.
- The backslash (\) indicates an escape character, and the special character following the backslash (\) indicates the special character itself. For example, \\ indicates the backslash (\) and \" indicates the quotation mark (").

- The double quotation marks ("") indicate that data enclosed is encapsulated in string format. Data without or outside the double quotation marks is encapsulated in hexadecimal format.
- Strings in ASCII format can contain 0 to 9, a to z, A to Z, and the following symbols: !, @, #, $, %, ^, &, *, (), _, +, |, -, =, \, [], {}, ;, :, '", /, ?, ., ,, <>, `.
- For characters %\" in ASCII format, add the prefix (\) in front of the characters. In ASCII format, only keywords and several specific symbols are converted and other data remains unchanged.
- If there is no escape character '%' in front of '%' in configuration commands, the key value in the information field must be added behind. Otherwise, the configuration is incorrect and an error is prompted. If the character '\' needs to be configured, enter "\\".
- For strings in hexadecimal format, digits are encapsulated into the option in hexadecimal notation. When hexadecimal data is used, strings begin with 0X or 0x. When the number of valid characters in the hexadecimal data is an odd, add one 0 to the frontmost. When decimal data is used, the data ranges from 0 to 255 and occupies one byte. You can use spaces to enter multiple pieces of decimal data consecutively.
- Blank characters in hexadecimal notation are ignored.

Examples

The following example sets the value of **Remote ID** to the device name and local host MAC address in ASCII format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option remote-id format user-defined
"%devicename %sysmac"
```

The following example sets the value of **Remote ID** to the local host MAC address in hexadecimal format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay option remote-id format user-defined %sysmac
```

Notifications

When the padding format of a keyword is incorrect (for example, **%portname** can be padded only in ASCII format), the following notification will be displayed:

```
% Format of Keyword unmatched.
```

When a keyword fails to be matched, the following notification will be displayed:

```
% User defined string include bad keyword.
```

When a keyword fails to be identified, the following notification will be displayed:

```
% DHCP6 RELAY could not parse the user defined string.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 dhcp relay option remote-id enable

1.16 ipv6 dhcp relay source

Function

Run the **ipv6 dhcp relay source** command to configure the source interface of a DHCPv6 relay agent.
Run the **no** form of this command to remove this configuration.
No source interface is configured for a DHCP relay agent by default.

Syntax

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *ipv6-address* | *interface-type interface-number* }

no ipv6 dhcp relay source

Parameter Description

source-ip-address: Sets the source IP address.

gateway-address: Sets the gateway address.

ipv6-address: IPv6 address of the source interface.

interface-type interface-number: Source interface type and number.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

The source interface definition function supports the following types of addresses:

- Source IP address: The source IP address field in DHCPv6 relay packets is changed.
- Gateway address: The source IP address and link address fields in DHCPv6 relay packets are changed.

The source interface definition function can be configured in global configuration mode and interface configuration mode. The source interface definition type in interface configuration mode is prior to that in global configuration mode. In the same configuration mode, the last configured source interface definition type prevails.

Caution

- When the source interface definition parameter uses IPv6 address, it cannot be set to a multicast address, local link address, site address, unconfigured address (with all 0s), or local loopback address.
- When the source interface definition parameter is the interface index, the interface must be an L3 interface. When the specified interface changes to a non-L3 interface, the configuration of the source interface definition function is deleted from this interface.

- When the source interface definition parameter is the interface index, if multiple IPv6 addresses are configured for the specified interface, the minimum global unicast address is used. If no global unicast address is configured for the interface, the current configuration does not take effect and packets are forwarded in default manner.

Examples

The following example enables the source interface definition function on SVI 1, sets the definition type to gateway address, and sets the definition parameter type to IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 dhcp relay source gateway-address 1000::1
```

The following example enables the source interface definition function on all interfaces, sets the definition type to source IP address, and sets the definition parameter type to interface index.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp relay source source-ip-address loopback 0
```

Notifications

When the source interface definition parameter is IPv6 address, but a multicast address, site address, unconfigured address, loopback address, or local link address is configured, the following notification will be displayed:

```
input invalid ipv6 address.
```

When the source interface definition parameter is interface index, but the specified interface is a non-L3 interface, the following notification will be displayed:

```
The specify interface(ifx_id) is not in layer3.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp relay source**

1.17 ipv6 dhcp server

Function

Run the **ipv6 dhcp server** command to enable the DHCPv6 Server function on an interface.

Run the **no** form of this command to disable this feature.

The DHCPv6 Server function is disabled by default.

Syntax

ipv6 dhcp server *pool-name* [**rapid-commit**] [**preference** *preference-value*]

no ipv6 dhcp server

Parameter Description

pool-name: DHCPv6 address pool name.

rapid-commit: Allows two-way message exchanges.

preference *preference-value*: Configures the priority of the ADVERTISE message. The range is from 0 to 255, and the default value is **0**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This function can be configured only on L3 interfaces.

After the **rapid-commit** parameter is configured, a DHCPv6 server can use the two-way message exchange mechanism to assign an address prefix and other configurations to a DHCPv6 client. That is, if the SOLICIT message from a client contains the **Rapid-Commit** option, the DHCPv6 server directly returns a REPLY message.

If **preference** is set to a non-zero value, the ADVERTISE message sent by the DHCPv6 server contains the **Preference** option. The **Preference** option affects DHCPv6 server selection of a client. A larger *preference-value* value indicates a higher priority. If a client receives an ADVERTISE message in which the **Preference** option is set to **255**, the client immediately sends a REQUEST message to the DHCPv6 server to obtain configurations.

The DHCPv6 Server, DHCPv6 Client, and DHCPv6 Relay functions are mutually exclusive, and only one function can be configured on an interface at a time.

Examples

The following example enables the DHCPv6 Server function on GigabitEthernet 0/1 and creates a DHCPv6 address pool named **pool1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp server pool1
```

Notifications

When the DHCPv6 Server function fails to be enabled, the following notification will be displayed:

```
Failed to start DHCPv6 interface, please try again.
```

When the configured address pool name is too long, the following notification will be displayed:

```
Pool name length should not be larger than 31.
```

When initialization is not completed due to insufficient memory, the following notification will be displayed:

```
Failed to initiate DHCPv6 interface, please try again
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp interface**

1.18 ipv6 local pool

Function

Run the **ipv6 local pool** command to configure a local prefix pool for the PD service of a DHCPv6 server.

Run the **no** form of this command to remove this configuration.

No local prefix pool is configured for the PD service of a DHCPv6 server by default.

Syntax

ipv6 local pool *pool-name prefix/prefix-length assigned-length*

no ipv6 local pool *pool-name*

Parameter Description

pool-name: Name of local prefix pool.

prefix/prefix-length: Prefix and prefix length.

assigned-length: Length of the prefix assigned to a DHCPv6 client. The range is from 0 to 128.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to create a local prefix pool. If a DHCPv6 server needs to implement local PD, run the **prefix-delegation pool** command to specify a local prefix pool. Then, the DHCPv6 server assigns prefixes from the specified local prefix pool.

Examples

The following example sets the name of the local prefix pool for PD of a DHCPv6 server to **client-prefix-pool**, sets the prefix to **2001::db8::/64**, and sets the length of prefixes to be assigned to clients to **80**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 local pool client-prefix-pool 2001::db8::/64 80
```

Notifications

When the length of the specified prefix pool name exceeds the limit, the following notification will be displayed:

```
Maximum pool name length is 31.
```

When the length of the specified prefix exceeds the limit, the following notification will be displayed:

```
Prefix length must be in the range [1,128] or [128, 128].
```

When the length of a prefix assigned to a client exceeds the limit (less than the prefix length of the local prefix pool or greater than the address length), the following notification will be displayed:

```
Assign length must be in the range [x,128] or [128,128].
```

When the difference between the length of the specified prefix and that of a prefix assigned to a client exceeds 16 bits, the following notification will be displayed:

```
Assign length minus prefix length must be not more than 16.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 local pool**
- **prefix-delegation pool**

1.19 option52

Function

Run the **option52** command to configure the IPv6 address of a Control and Provisioning of Wireless Access Points (CAPWAP) access controller (AC) specified on a DHCPv6 server.

Run the **no** form of this command to remove this configuration.

The AC IPv6 address information is not configured by default.

Syntax

option52 *ipv6-address*

no option52 *ipv6-address*

Parameter Description

ipv6-address: IPv6 address of a CAPWAP AC.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

You can run this command multiple times to specify multiple IPv6 addresses for a CAPWAP AC. A new CAPWAP AC IPv6 address does not overwrite an old one. A maximum of 10 IPv6 addresses can be configured.

Examples

The following example sets the IPv6 address of the CAPWAP AC specified on a DHCPv6 server to **2008:1::1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# option52 2008:1::1
```

Notifications

When the number of configured addresses in Option 52 exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 option52 address limit for each pool, 10.
```

When Option 52 address configuration fails, the following notification will be displayed:

```
Failed to configure option52 address, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.20 prefix-delegation

Function

Run the **prefix-delegation** command to configure prefixes for statically bound addresses on a DHCPv6 server.

Run the **no** form of this command to remove this configuration.

No prefix is configured for a statically bound address on a DHCPv6 server by default.

Syntax

prefix-delegation *ipv6-address/prefix-length client-DUID* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

Parameter Description

ipv6-address/prefix-length: IPv6 address or prefix length.

client-DUID: DUID of a client.

lifetime: Sets the valid time of an address prefix to be assigned to a client.

valid-lifetime: Valid time of a prefix to be assigned to a client, in seconds. The range is from 60 to 4294967295. The default value is **3600**, that is, 1 hour.

preferred-lifetime: Time during which a prefix is still preferentially assigned to a client, in seconds. The range is from 60 to 4294967295. The default value is **3600**, that is, 1 hour.

infinite: Configures permanent lease.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

You can run this command to manually configure a prefix list for an IA_PD of a client and specify the valid time of these prefixes.

The *client-DUID* parameter specifies the client to which an address prefix is to be assigned. The address prefix will be assigned to the first IA_PD of the client.

After receiving a REQUEST message for an address prefix from the client, the DHCPv6 server checks whether a static binding is available. If yes, the DHCPv6 server directly returns the static binding. If not, the DHCPv6 server assigns an address prefix from another prefix source.

Examples

The following example sets the address prefix to be assigned to a client (with the DUID of 0003000100d0f82233ac) in DHCPv6 address pool pool1 to **2008:2::/64**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#ipv6 dhcp pool pool1
Hostname(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac
```

Notifications

When the specified DUID is incorrect, the following notification will be displayed:

```
DUID string length must not be odd number or exceed 128.
```

When the number of configured prefixes for statically bound addresses on a DHCPv6 server exceeds the limit, the following notification will be displayed:

```
Reach dhcpv6 static IAPD binding limit 1024.
```

When prefixes for statically bound addresses fail to be configured, the following notification will be displayed:

```
Failed to configure prefix delegation, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.21 prefix-delegation pool

Function

Run the **prefix-delegation pool** command to configure a local prefix pool on a DHCPv6 server.

Run the **no** form of this command to remove this configuration.

No local prefix pool is configured for a DHCPv6 server by default.

Syntax

prefix-delegation pool *pool-name* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

no prefix-delegation pool *pool-name*

Parameter Description

pool-name: User-defined name of a local prefix pool.

lifetime: Sets the valid time of a prefix to be assigned to a client.

valid-lifetime: Valid time of a prefix to be assigned to a client, in seconds. The range is from 60 to 4294967295. The default value is **3600**, that is, 1 hour.

preferred-lifetime: Time during which a prefix is still preferentially assigned to a client, in seconds. The range is from 60 to 4294967295. The default value is **3600**, that is, 1 hour.

infinite: Configures permanent lease.

Command Modes

DHCPv6 address pool configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a prefix pool for a DHCPv6 server to assign prefixes to clients. You can run the **ipv6 local pool** command to create a prefix pool.

When receiving a prefix request from a client, the DHCPv6 server selects an available prefix from the prefix pool and assigns the prefix to the client. When the client no longer needs this prefix, the DHCPv6 server reclaims it.

Examples

The following example configures a local prefix pool named **client-prefix-pool** for clients in DHPCv6 address pool pool1, sets the valid time for a client to use an assigned prefix to 2000s, and sets the time during which a prefix is still preferentially assigned to a client to 1000s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000
```

Notifications

When the value of *valid-lifetime* is smaller than that of *preferred-lifetime*, the following notification will be displayed:

```
Preferred lifetime must not exceed valid lifetime.
```

When prefixes for statically bound addresses fail to be configured, the following notification will be displayed:

```
Failed to configure prefix delegation, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp pool**

1.22 show ipv6 dhcp

Function

Run the **show ipv6 dhcp** command to display the DUID of a DHCPv6 device.

Syntax

show ipv6 dhcp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The DHCPv6 server, client, and relay on the same device share one DUID.

Examples

The following example displays the DUID of the current device.

```
Hostname> enable
Hostname# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Table 1-3 Output Fields of the show ipv6 dhcp Command

Field	Description

This device's DHCPv6 unique identifier (DUID)	Unique identifier of a DHCPv6 device

Notifications

N/A

Platform Description

N/A

1.23 show ipv6 dhcp binding

Function

Run the **show ipv6 dhcp binding** command to display address bindings on a DHCPv6 server.

Syntax

show ipv6 dhcp binding [*ipv6-address*]

Parameter Description

ipv6-address: IPv6 address or prefix.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *ipv6-address* parameter is not configured, all bindings between prefixes and IA_NA addresses dynamically assigned to clients and clients are displayed. If the *ipv6-address* parameter is configured, only bindings of the specified address are displayed.

Examples

The following example displays all address bindings on a DHCPv6 server.

```
Hostname> enable
Hostname# show ipv6 dhcp binding
Client  DUID: 00:03:00:01:00:d0:f8:22:33:ac
  IAPD: iaid 0, T1 1800, T2 2880
  Prefix: 2001:20::/72
  preferred lifetime 3600, valid lifetime 3600
  expires at Jan 1 2008 2:23 (3600 seconds)
```

Table 1-4 Output Fields of the show ipv6 dhcp binding Command

Field	Description
Client DUID	DUID of a client.

IAPD	Bound IA type, which can also be IA_NA. It includes the following information: ● Iaid: IA ID. ● T1: T1 value of the IA. A client needs to send a RENEW message to update the address lease after T1. ● T2: T2 value of the IA. If the update is not complete within T2, the client needs to send another RENEW message.
Prefix	Prefix assigned to a client.
preferred lifetime	Time during which the prefix is still preferentially assigned to a client.
valid lifetime	Valid time of the prefix.
expires at	Time when the prefix expires.

Notifications

N/A

Platform Description

N/A

1.24 show ipv6 dhcp conflict

Function

Run the **show ipv6 dhcp conflict** command to display conflicted addresses on a DHCPv6 server.

Syntax

show ipv6 dhcp conflict

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display all conflicted addresses on a DHCPv6 server.

Examples

The following example displays conflicted addresses on a DHCPv6 server.

```
Hostname> enable
Hostname# show ipv6 dhcp conflict
```

```
2008:50::2   declined
2108:50::2   declined
2008:50::3   declined
2008:50::4   declined
2108:50::4   declined
2008:50::5   declined
```

Table 1-5 Output Fields of the show ipv6 dhcp conflict Command

Field	Description
2008:50::2 declined	Conflict address

Notifications

N/A

Platform Description

N/A

1.25 show ipv6 dhcp interface

Function

Run the **show ipv6 dhcp interface** command to display DHCPv6 interfaces.

Syntax

show ipv6 dhcp interface [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *interface-type interface-number* parameter is not configured, all DHCPv6 interfaces are displayed. If the *interface-type interface-number* parameter is configured, only the specified interface is displayed.

Examples

The following example displays all interfaces on a DHCPv6 server.

```
Hostname> enable
Hostname# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool: dhcp-pool
```

```
Rapid-Commit: disable
```

Table 1-6 Output Fields of the show ipv6 dhcp interface Command

Field	Description
xxx is in yyy mode	The xxx interface works in yyy mode. The values of yyy include: ● **Client**: The interface works in client mode. ● **Relay**: The interface works in relay mode. ● **Server**: The interface works in server mode.
Server pool	When the DHCPv6 Server function is enabled on an interface, the address pool name of the interface is displayed.
Rapid-Commit	Indicates whether the **Rapid-Commit** option is enabled. The values include: ● **enable**: Two-way message exchange is enabled. ● **disable**: Two-way message exchange is disabled.

Notifications

N/A

Platform Description

N/A

1.26 show ipv6 dhcp pool

Function

Run the **show ipv6 dhcp pool** command to display DHCPv6 address pools.

Syntax

show ipv6 dhcp pool [*pool-name*]

Parameter Description

pool-name: User-defined name of a DHCPv6 address pool.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *pool-name* parameter is not configured, all DHCPv6 address pools are displayed. If the *pool-name* parameter is configured, only the specified address pool is displayed.

Examples

The following example displays all DHCPv6 address pools.

```
Hostname> enable
Hostname# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com
```

Table 1-7 Output Fields of the show ipv6 dhcp pool Command

Field	Description
DHCPv6 pool	User-defined name of DHCPv6 address pool
DNS Server	DNS server address to be assigned to a client
Domain name	Domain name to be assigned to a client

Notifications

N/A

Platform Description

N/A

1.27 show ipv6 dhcp relay agent

Function

Run the **show ipv6 dhcp relay agent** command to display source interfaces on a DHCPv6 relay agent.

Syntax

show ipv6 dhcp relay agent { *ipv6-address* | * }

Parameter Description

ipv6-address: IPv6 address or prefix. When this parameter is configured, the source interface of a specified link address is displayed.

*: All source interfaces and the corresponding link addresses.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the source interfaces and the corresponding link addresses in request packets received by a DHCPv6 relay agent.

Examples

The following example displays all source interfaces and corresponding link addresses on a DHCPv6 relay agent.

```
Hostname> enable
Hostname# show ipv6 dhcp relay agent *
Link local address          l2 interface
---------------
```

Table 1-8 Output Fields of the show ipv6 dhcp relay agent Command

Field	Description
Link local address	Link address
l2 interface	Index of an L2 interface that receives request packets

Notifications

N/A

Platform Description

N/A

1.28 show ipv6 dhcp relay destination

Function

Run the **show ipv6 dhcp relay destination** command to display destination addresses on a DHCPv6 relay agent.

Syntax

show ipv6 dhcp relay destination { **all** | *interface-type interface-number* }

Parameter Description

all: Displays all configured destination addresses and interfaces.

interface-type interface-number: Type and number of the interface whose configured destination addresses and interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the destination address and interface for forwarding DHCPv6 packets received from clients on an interface with the DHCPv6 Relay service enabled.

Examples

The following example displays the destination addresses of all DHCPv6 relay agents.

```
Hostname> enable
Hostname# show ipv6 dhcp relay destination all
Interface:VLAN 1
Destination address(es)              Output Interface
3001::2
ff02::1:2                           VLAN 2
```

Table 1-9 Output Fields of the show ipv6 dhcp relay destination Command

Field	Description
Interface	Interface on which the DHCPv6 Relay service is enabled
Destination address(es)	Destination address
Output Interface	Outbound interface of packets

Notifications

N/A

Platform Description

N/A

1.29 show ipv6 dhcp relay source

Function

Run the **show ipv6 dhcp relay source** command to display the source interface definition configuration on a DHCPv6 relay agent.

Syntax

show ipv6 dhcp relay source

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the source interface definition configuration of the DHCPv6 relay on the current device.

```
Hostname> enable
Hostname#show ipv6 dhcp relay source
Interface-Name         Source-Intf-Type      Source-Intf-Parameter
Global                Source Address        VLAN 10
VLAN 1                Gateway Address       1000::1
GigabitEthernet 0/7     Source Address        3000::1:1
```

Table 1-10 Output Fields of the show ipv6 dhcp relay source Command

Field	Description
Interface-Name	Name of the interface that is configured with the source interface definition function. It is fixed to **Global** in global configuration mode.
Source-Intf-Type	Source interface definition type.
Source-Intf-Parameter	Source interface definition parameter.

Notifications

N/A

Platform Description

N/A

1.30 show ipv6 dhcp relay statistics

Function

Run the **show ipv6 dhcp relay statistics** command to display statistics of different types of packets on a DHCPv6 relay agent.

Syntax

show ipv6 dhcp relay statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics of different types of packets on a DHCPv6 relay agent.

```
Hostname> enable
Hostname# show ipv6 dhcp relay statistics
Packets dropped             :  2
   Error                   :  2
   Excess of rate limit     :  0
Packets received            :  28
   SOLICIT                 :  0
   REQUEST                 :  0
   CONFIRM                 :  0
   RENEW                   :  0
   REBIND                  :  0
   RELEASE                 :  0
   DECLINE                 :  0
   INFORMATION-REQUEST      :  14
   RELAY-FORWARD           :  0
   RELAY-REPLY             :  14
Packets sent                :  16
   ADVERTISE               :  0
   RECONFIGURE             :  0
   REPLY                   :  8
   RELAY-FORWARD           :  8
   RELAY-REPLY             :  0
```

Table 1-11 Output Fields of the show ipv6 dhcp relay statistics Command

Field	Description
Packets dropped	Total number of unprocessed packets discarded
Error	Number of error packets discarded
Excess of rate limit	Number of packets discarded due to an insufficient processing capacity of the device
Packets received	Total number of normal DHCPv6 packets received
SOLICIT	Number of SOLICIT packets
REQUEST	Number of REQUEST packets
CONFIRM	Number of CONFIRM packets
RENEW	Number of RENEW packets
REBIND	Number of REBIND packets

Field	Description
RELEASE	Number of RELEASE packets
DECLINE	Number of DECLINE packets
INFORMATION-REQUEST	Number of INFORMATION-REQUEST packets
RELAY-FORWARD	Number of RELAY-FORWARD packets
RELAY-REPLY	Number of RELAY-REPLY packets
Packets sent	Total number of normal DHCPv6 packets sent
ADVERTISE	Number of ADVERTISE packets
RECONFIGURE	Number of RECONFIGURE packets
REPLY	Number of REPLY packets
RELAY-FORWARD	Number of RELAY-FORWARD packets
RELAY-REPLY	Number of RELAY-REPLY packets

Notifications

N/A

Platform Description

N/A

1.31 show ipv6 dhcp server statistics

Function

Run the **show ipv6 dhcp server statistics** command to displays DHCPv6 server statistics.

Syntax

show ipv6 dhcp server statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays DHCPv6 server statistics.

```
Hostname> enable
Hostname# show ipv6 dhcp server statistics
DHCPv6 server statistics:
Packet statistics:
DHCPv6 packets received:           7
Solicit received:                 7
Request received:                 0
Confirm received:                 0
Renew received:                   0
Rebind received:                  0
Release received:                 0
Decline received:                 0
Relay-forward received:            0
Information-request received:       0
Unknown message type received:      0
Error message received:            0
DHCPv6 packet sent:               0
Advertise sent:                   0
Reply sent:                       0
Relay-reply sent:                  0
Send reply error:                  0
Send packet error:                 0
Binding statistics:
Bindings generated:                0
IAPD assigned:                    0
IANA assigned:                    0
Configuration statistics:
DHCPv6 server interface:           1
DHCPv6 pool:                      0
DHCPv6 iapd binding:               0
```

Table 1-12 Output Fields of the show ipv6 dhcp server statistics Command

Field	Description
Packet statistics	Statistics about the packet quantity
DHCPv6 packets received	Number of packets received
Solicit received	Number of SOLICIT packets received
Request received	Number of REQUEST packets received
Confirm received	Number of CONFIRM packets received
Renew received	Number of RENEW packets received

Rebind received	Number of REBIND packets received
Release received	Number of RELEASE packets received
Decline received	Number of DECLINE packets received
Relay-forward received	Number of RELAY-FORWARD packets received
Information-request received	Number of INFORMATION-REQUEST packets received
Unknown message type received	Number of unknown packets received
Error message received	Number of error packets received
DHCPv6 packet sent	Number of packets sent
Advertise sent	Number of ADVERTISE packets sent
Reply sent	Number of REPLY packets sent
Relay-reply sent	Number of RELAY-REPLY packets sent
Send reply error	Number of error response packets sent
Send packet error	Number of error packets sent
Binding statistics	Statistics about bindings ● **Bindings generated**: Number of generated bindings ● **IAPD assigned**: Number of assigned IA_PDs ● **IANA assigned**: Number of assigned IA_NAs
Bindings generated	Number of assigned entries
IAPD assigned	Number of prefix entries
IANA assigned	Number of address entries
Configuration statistics	Statistics about configurations ● **DHCPv6 Server interface**: Number of interfaces enabled with the DHCPv6Server function ● **DHCPv6 pool**: Number of configured pools ● **DHCPv6 iapd binding**: Number of configured prefixes for statically bound addresses

Notifications

N/A

Platform Description

N/A

1.32 show ipv6 local pool

Function

Run the **show ipv6 local pool** command to display local prefix pool configuration and usage on the current device.

Syntax

show ipv6 local pool [*pool-name*]

Parameter Description

pool-name: Name of the local prefix pool.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display local prefix pool configuration and usage on the current device.

Examples

The following example displays configuration and usage of all local prefix pools.

```
Hostname> enable
Hostname# show ipv6 local pool
Pool               Prefix                  Free          In use
client-prefix-pool   2001:db8::/64            65536          0
```

Table 1-13 Output Fields of the show ipv6 local pool Command

Field	Description
Pool	Name of the local prefix pool
Prefix	Prefix and prefix length
Free	Available prefixes
In use	Prefixes being used

The following example displays the local prefix pool for the address pool client-prefix-pool.

```
Hostname# show ipv6 local pool client-prefix-pool
Prefix is 2001:db8::/64 assign /80 prefix
1 entries in use, 65535 available
Prefix                                              Interface
2001:db8::/80                                        GigabitEthernet 0/0
```

Table 1-14 Output Fields of the show ipv6 local pool Command

Field	Description
Prefix	Assigned prefix and prefix length.
x entries in use	x prefixes are being used.
y available	y prefixes are available.
Interface	Interface over which a prefix is assigned.

Notifications

N/A

Platform Description

N/A

1 DHCPv6 Client Commands

Command	Function
clear ipv6 dhcp client	Restart the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client function on an interface.
ipv6 dhcp client ia	Enable the DHCPv6 Client function on an interface and request an identity association non-temporary address (IA_NA) address.
ipv6 dhcp client pd	Enable the DHCPv6 Client function on an interface and request an address prefix.
show ipv6 dhcp	Display the DHCP Unique Identifier (DUID) of a device.
show ipv6 dhcp interface	Display DHCPv6 interfaces.

1.1 clear ipv6 dhcp client

Function

Run the **clear ipv6 dhcp client** command to restart the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client function on an interface.

Syntax

clear ipv6 dhcp client *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to restart the DHCPv6 Client function on an interface to request configurations from a DHCPv6 server again.

Examples

The following example restarts the DHCPv6 Client service on Switch Virtual Interface (SVI) 1.

```
Hostname> enable
Hostname# clear ipv6 dhcp client vlan 1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ipv6 dhcp client ia

Function

Run the **ipv6 dhcp client ia** command to enable the DHCPv6 Client function on an interface and request an identity association non-temporary address (IA_NA) address.

Run the **no** form of this command to remove this configuration.

The DHCPv6 Client function and IA_NA address requesting are disabled by default.

Syntax

ipv6 dhcp client ia [**rapid-commit**]

no ipv6 dhcp client ia

Parameter Description

rapid-commit: Allows two-message exchange. If this keyword is configured, the SOLICIT message from the client contains the **Rapid-commit** option.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the DHCPv6 Client function is disabled on an interface, this command is used to enable the DHCPv6 Client function on the interface.

Examples

The following example enables the DHCPv6 Client function on GigabitEthernet 0/1 and requests an IA_NA address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client ia
```

Notifications

When the DHCPv6 Client function fails to be enabled, the following notification will be displayed:

```
Failed to configure DHCPv6 interface, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp interface**

1.3 ipv6 dhcp client pd

Function

Run the **ipv6 dhcp client pd** command to enable the DHCPv6 Client function on an interface and request an address prefix.

Run the **no** form of this command to remove this configuration.

Address prefix requesting is not configured by default.

Syntax

ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

no ipv6 dhcp client pd

Parameter Description

prefix-name: General IPv6 prefix.

rapid-commit: Allows two-message exchange. If this keyword is configured, the SOLICIT message from the client contains the **Rapid-commit** option.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the DHCPv6 Client function is disabled on an interface, this command is used to enable the DHCPv6 Client function on the interface.

After this command is executed, the device sends a prefix request to a DHCPv6 server. After receiving the prefix, the client saves the prefix to the general IPv6 prefix pool. In this way, other commands and applications can use this prefix.

Examples

The following example enables the DHCPv6 Client function on GigabitEthernet 0/1 and requests an address prefix.

```
Hostname> enable
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client pd pd_name
```

Notifications

When the DHCPv6 Client function fails to be enabled, the following notification will be displayed:

```
Failed to configure DHCPv6 interface, please try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 dhcp interface**

1.4 show ipv6 dhcp

Function

Run the **show ipv6 dhcp** command to display the DHCP Unique Identifier (DUID) of a device.

Syntax

show ipv6 dhcp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The DHCPv6 server, client, and relay on the same device share one DUID.

Examples

The following example displays the DUID of a device.

```
Hostname> enable
Hostname# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Table 1-1 Output Fields of the show ipv6 dhcp interface Command

Field	Description
This device's DHCPv6 unique identifier (DUID)	Unique identifier of a DHCPv6 device

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show ipv6 dhcp interface

Function

Run the **show ipv6 dhcp interface** command to display DHCPv6 interfaces.

Syntax

show ipv6 dhcp interface [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *interface-type interface-number* parameter is not configured, information about all DHCPv6 interfaces is displayed. If the *interface-type interface-number* parameter is configured, only information about the specified DHCPv6 interface is displayed.

Examples

The following example displays interfaces on a DHCPv6 server.

```
Hostname> enable
Hostname# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool: dhcp-pool
  Rapid-Commit: disable
```

Table 1-2 Output Fields of the show ipv6 dhcp interface Command

Field	Description
xxx is in yyy mode	The xxx interface works in yyy mode. The values of yyy include: ● **Client**: The interface works in client mode. ● **Relay**: The interface works in relay mode. ● **Server**: The interface works in server mode.
Server pool	When the DHCPv6 Server function is enabled on an interface, the address pool name of the interface is displayed.
Rapid-Commit	Indicates whether the Rapid-Commit option is enabled. The values include: ● **enable**: Two-way message exchange is enabled. ● **disable**: Two-way message exchange is disabled.

2. The following example displays interfaces on a DHCPv6 client.

```
Hostname> enable
Hostname# show ipv6 dhcp interface
GigabitEthernet 0/1 is in client mode
  Rapid-Commit: disable
```

Table 1-3 Output Fields of the show ipv6 dhcp interface Command

Field	Description
xxx is in yyy mode	The xxx interface works in yyy mode. The values of yyy include: ● **Client**: The interface works in client mode. ● **Relay**: The interface works in relay mode. ● **Server**: The interface works in server mode.
Rapid-Commit	Indicates whether the Rapid-Commit option is enabled. The values include: ● **enable**: Two-way message exchange is enabled. ● **disable**: Two-way message exchange is disabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 DHCPv6 Snooping Commands

Command	Function
clear ipv6 dhcp snooping binding	Clear all dynamic user information in the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Snooping binding database.
clear ipv6 dhcp snooping prefix	Clear all user information in the DHCPv6 Snooping prefix database.
clear ipv6 dhcp snooping statistics	Clear statistics about DHCPv6 packets processed by DHCPv6 Snooping.
ipv6 dhcp snooping	Enable DHCPv6 Snooping globally.
ipv6 dhcp snooping database write-delay	Write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.
ipv6 dhcp snooping database write-to-flash	Write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.
ipv6 dhcp snooping information option	Add Option 18 or 37 to DHCPv6 request packets.
ipv6 dhcp snooping information option format remote-id	Set the Remote ID sub-option to a user-defined string or the host name when Option 37 is in extended padding mode.
ipv6 dhcp snooping filter-dhcp-pkt	Configure an interface to filter all DHCPv6 request packets.
ipv6 dhcp snooping link-detection	Clear dynamically bound entries on an interface in linkdown state.
ipv6 dhcp snooping trust	Configure an interface as a DHCPv6 Snooping trusted port.
ipv6 dhcp snooping vlan	Enable DHCPv6 Snooping on a VLAN.
ipv6 dhcp snooping vlan information option change-vlan-to vlan	Change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.
ipv6 dhcp snooping vlan information option format-type interface-id string	Set the Interface ID to a user-defined string for forwarding when Option 18 is in extended padding mode.

renew ipv6 dhcp snooping database	Import information in a flash memory to the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping	Display DHCPv6 Snooping configurations.
show ipv6 dhcp snooping vlan	Display VLANs to which DHCPv6 Snooping does not take effect.
show ipv6 dhcp snooping binding	Display dynamic user information in the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping prefix	Display user information in the DHCPv6 Snooping prefix database.
show ipv6 dhcp snooping statistics	Display statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.
show ipv6 dhcp snooping packet	Display statistics about packets related to the DHCPv6 Snooping function.

1.1 clear ipv6 dhcp snooping binding

Function

Run the **clear ipv6 dhcp snooping binding** command to clear all dynamic user information in the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Snooping binding database.

Syntax

clear ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address of a user to be deleted.

mac-address: Media access control (MAC) address of a user to be deleted.

vlan *vlan-id*: Specifies the ID of the virtual local area network (VLAN) of a user to be deleted.

interface *interface-type interface-number*: Specifies the interface of a user to be deleted.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After this command is run, all DHCPv6 users who access an interface with DHCPv6 Source Guard enabled need to re-apply for IPv6 addresses. Otherwise, they cannot access the Internet.

Examples

The following example clears all dynamic user information in the DHCPv6 Snooping binding database.

```
Hostname> enable
Hostname# clear ipv6 dhcp snooping binding
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 dhcp snooping prefix

Syntax

Run the **clear ipv6 dhcp snooping prefix** command to clear all user information in the DHCPv6 Snooping prefix database.

Syntax

clear ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address of a user to be deleted.

mac-address: MAC address of a user to be deleted.

vlan *vlan-id*: Specifies the ID of the VLAN of a user to be deleted.

interface *interface-type interface-number*: Specifies the interface of a user to be deleted.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all user information in the DHCPv6 Snooping prefix database.

```
Hostname> enable
Hostname# clear ipv6 dhcp snooping prefix
```

Notifications

N/A

Platform Description

N/A

1.3 clear ipv6 dhcp snooping statistics

Function

Run the **clear ipv6 dhcp snooping statistics** command to clear statistics about DHCPv6 packets processed by DHCPv6 Snooping.

Syntax

clear ipv6 dhcp snooping statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics about DHCPv6 packets processed by DHCPv6 Snooping.

```
Hostname> enable
Hostname# clear ipv6 dhcp snooping statistics
```

Notifications

N/A

Platform Description

N/A

1.4 ipv6 dhcp snooping

Function

Run the **ipv6 dhcp snooping** command to enable DHCPv6 Snooping globally.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

DHCPv6 Snooping is disabled globally by default.

Syntax

ipv6 dhcp snooping

no ipv6 dhcp snooping

default ipv6 dhcp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables DHCPv6 Snooping globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 dhcp snooping database write-delay

Function

Run the **ipv6 dhcp snooping database write-delay** command to write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.

Run the **no** form of this command to remove this configuration.

The function of writing all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time is not configured by default.

Syntax

ipv6 dhcp snooping database write-delay *time*

no ipv6 dhcp snooping database write-delay

Parameter Description

time: Period for saving database records, in seconds. The value range is from 600 to 86400.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time. This prevents binding information loss after a device restarts, there is no need to re-obtain IPv6 addresses to restore communication.

Note

A high saving frequency reduces the lifespan of the flash memory.

Examples

The following example writes all dynamic user information in the DHCPv6 Snooping binding database to a flash memory every 3600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping database write-delay 3600
```

Notifications

N/A

Common Errors

The configured period exceeds the limit.

Platform Description

N/A

Related Commands

- **ipv6 dhcp snooping database write-to-flash**

1.6 ipv6 dhcp snooping database write-to-flash

Function

Run the **ipv6 dhcp snooping database write-to-flash** command to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

Syntax

ipv6 dhcp snooping database write-to-flash

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

Examples

The following example writes dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping database write-to-flash
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 dhcp snooping database write-delay

1.7 ipv6 dhcp snooping information option

Function

Run the **ipv6 dhcp snooping information option** command to add Option 18 or 37 to DHCPv6 request packets.

Run the **no** form of this command to remove this configuration.

Option 18 or 37 is not added to DHCPv6 request packets by default.

Syntax

ipv6 dhcp snooping information option [**standard-format**]

no ipv6 dhcp snooping information option [**standard-format**]

Parameter Description

standard-format: Uses the standard padding format for Option 18 or 37.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to add Option 18 or 37 to DHCPv6 request packets, so that a DHCP server can assign addresses based on Option 18 or 37.

When Option 18 or 37 is enabled, the extended padding mode is used by default.

Caution

- Option 18 or 37 for DHCPv6 Snooping and DHCP Relay are mutually exclusive.
- In wireless access scenarios, the **Circuit ID** sub-option is fixed at **0** in both standard padding and extended padding modes of Option 18.

Examples

The following example adds Option 18 or 37 to DHCPv6 request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping information option
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 dhcp snooping information option format remote-id**
- **ipv6 dhcp snooping vlan information option change-vlan-to vlan**
- **ipv6 dhcp snooping vlan information option format-type interface-id string**

1.8 ipv6 dhcp snooping information option format remote-id

Function

Run the **ipv6 dhcp snooping information option format remote-id** command to set the **Remote ID** sub-option to a user-defined string or the host name when Option 37 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 37 is in extended padding mode, **Remote ID** is not set to a user-defined string or host name by default.

Syntax

ipv6 dhcp snooping information option format remote-id { **hostname** | **string** *ascii-string* }

no ipv6 dhcp snooping information option format remote-id { **hostname** | **string** *ascii-string* }

Parameter Description

hostname: Sets **Remote ID** to the host name.

string *ascii-string*: Sets **Remote ID** to a user-defined string.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When Option 37 is enabled for DHCPv6 packets in extended padding mode, this command is used to customize the content of **Remote ID**.

Examples

The following example sets **Remote ID** to a host name when Option 37 is in extended padding mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping information option format remote-id hostname
```

Notifications

When the value of the *ascii-string* parameter exceeds 63 characters, the following notification will be displayed:

```
% Failed to execute command, because of "Remote-ID string cannot exceed 63 characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 dhcp snooping information option**

1.9 ipv6 dhcp snooping filter-dhcp-pkt

Function

Run the **ipv6 dhcp snooping filter-dhcp-pkt** command to configure an interface to filter all DHCPv6 request packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is configured to filter all DHCPv6 request packets by default.

Syntax

ipv6 dhcp snooping filter-dhcp-pkt

no ipv6 dhcp snooping filter-dhcp-pkt

default ipv6 dhcp snooping filter-dhcp-pkt

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to reject all DHCPv6 packets on an untrusted port, that is, to forbid all users on this port to apply for addresses via DHCPv6.

This command can be configured only on L2 switching ports, aggregation ports (APs), or encapsulation sub-interfaces.

Examples

The following example configures GigabitEthernet 0/1 to filter all DHCPv6 request packets sent to this interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping filter-dhcp-pkt
```

Notifications

When this command is configured on a DHCPv6 trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port, AP, or L2 encapsulation sub-interface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 dhcp snooping link-detection

Function

Run the **ipv6 dhcp snooping link-detection** command to clear dynamically bound entries on an interface in linkdown state.

Run the **no** form of this command to remove this configuration.

Dynamically bound entries on an interface in linkdown state are not cleared by default.

Syntax

ipv6 dhcp snooping link-detection

no ipv6 **dhcp snooping link-detection**

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears dynamically bound entries on an interface in linkdown state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping link-detection
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 dhcp snooping trust

Function

Run the **ipv6 dhcp snooping trust** command to configure an interface as a DHCPv6 Snooping trusted port.

Run the **no** form of this command to remove this configuration.

All interfaces are DHCPv6 Snooping untrusted ports by default.

Syntax

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure interfaces connected to legitimate DHCPv6 servers as trusted ports. DHCPv6 response packets received on trusted ports are forwarded normally, while those received on untrusted ports are discarded.

This command can be configured only on L2 switching ports, APs, and L2 encapsulation sub-interfaces.

Caution

Generally, uplink interfaces, that is, interfaces connected to trusted DHCPv6 servers are configured as trusted ports.

Examples

The following example configures GigabitEthernet 0/1 as a DHCPv6 Snooping trusted port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ipv6 dhcp snooping trust
```

Notifications

When an interface configured with other access security control options is configured as a DHCPv6 Snooping trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port or AP, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 dhcp snooping

1.12 ipv6 dhcp snooping vlan

Function

Run the **ipv6 dhcp snooping vlan** command to enable DHCPv6 Snooping on a VLAN.

Run the **no** form of this command to remove this configuration.

After DHCPv6 Snooping is enabled globally, it takes effect to all VLANs by default.

Syntax

ipv6 dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

no ipv6 dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

Parameter Description

vlan-range: Range of VLANs in which DHCPv6 Snooping takes effect. The value is a character string, for example 1, 3–5, 7, and 9–11.

vlan-min: Minimum ID of a VLAN to DHCPv6 Snooping takes effect. The value range is from 1 to 4094.

vlan-max: Maximum ID of a VLAN to DHCPv6 Snooping takes effect. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable or disable DHCPv6 Snooping for a specific VLAN. This function takes effect only when DHCPv6 Snooping is enabled globally.

Examples

The following example enables DHCPv6 Snooping for VLAN 1000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping vlan 1000
```

The following example enables DHCPv6 Snooping for VLAN 1 to VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping vlan 1-10
```

Notifications

When the configured VLAN ID is beyond the range of 1 to 4094, the following notification will be displayed:

```
% Failed to execute command, because of "Not supported vlan range".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv6 dhcp snooping vlan information option change-vlan-to vlan

Function

Run the **ipv6 dhcp snooping vlan information option change-vlan-to vlan** command to change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 18 is in extended padding mode, the padded VLAN is not changed to a specified VLAN by default.

Syntax

ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

no ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When Option 18 is enabled for DHCPv6 packets in extended padding mode, this command is used to change the padded VLAN to a specified VLAN.

Examples

The following example adds Option 18 to DHCPv6 request packets and changes VLAN 4094 in the **Interface ID** sub-option of Option 18 to VLAN 4093.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ipv6 dhcp snooping vlan 4094 information option change-vlan-to
vlan 4093
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 dhcp snooping information option**
- **ipv6 dhcp snooping vlan information option format-type interface-id string**

1.14 ipv6 dhcp snooping vlan information option format-type interface-id string

Function

Run the **ipv6 dhcp snooping vlan information option format-type interface-id string** command to set **the Interface ID** to a user-defined string for forwarding when Option 18 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 18 is in extended padding mode, **Interface ID** is not set to a user-defined string for forwarding by default.

Syntax

ipv6 dhcp snooping vlan *vlan-id* **information option format-type interface-id string** *ascii-string*

no ipv6 dhcp snooping vlan *vlan-id* **information option format-type interface-id string** *ascii-string*

Parameter Description

vlan-id: VLAN of DHCPv6 request packets.

ascii-string: User-defined **Interface ID** content. The value is a string of 3 to 63 bytes in ASCII format.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When DHCPv6 Option 18 is enabled in extended padding mode, this command is used to set **Interface ID** to a user-defined string.

Examples

The following example sets **Interface ID** to a port name when Option 18 is added to DHCPv6 request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ipv6 dhcp snooping vlan 4094 information option format-type
interface-id string port-name
```

Notifications

When the user-defined character string is not 3 to 63 characters, the following notification is displayed:

```
% Failed to execute command, because of "Interface-ID string must be 3 to 63 characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 dhcp snooping information option**
- **ipv6 dhcp snooping vlan information option change-vlan-to vlan**

1.15 renew ipv6 dhcp snooping database

Function

Run the **renew ipv6 dhcp snooping database** command to import information in a flash memory to the DHCPv6 Snooping binding database.

Syntax

renew ipv6 dhcp snooping database

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to import the information in a flash memory to the DHCPv6 Snooping binding database.

Caution

- Lease expiration records in the backup file are ignored.
- Only records that do not exist in the database are added.

Examples

The following example imports information in a flash memory to the DHCPv6 Snooping binding database.

```
Hostname> enable
Hostname# renew ipv6 dhcp snooping database
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 dhcp snooping database write-to-flash

1.16 show ipv6 dhcp snooping

Function

Run the **show ipv6 dhcp snooping** command to display DHCPv6 Snooping configurations.

Syntax

show ipv6 dhcp snooping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays DHCPv6 Snooping configurations.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping
DHCPv6 snooping status                 : ENABLE
DHCPv6 snooping database write-delay time : 0 seconds
DHCPv6 snooping binding-delay time       : 0 seconds
DHCPv6 snooping option18/37 status       : DISABLE
DHCPv6 snooping link detection          : DISABLE
Interface               Trusted    Filter DHCPv6
-----------------------    -------    -------------
GigabitEthernet 0/1        YES       DISABLE
```

Table 1-1 Output Fields of the show ipv6 dhcp snooping Command

Field	Description
DHCPv6 snooping status	Indicates whether DHCPv6 snooping is enabled globally
DHCPv6 snooping database write-delay time	Interval for writing data to a flash memory.
DHCPv6 snooping binding-delay time	Delayed time for adding dynamically generated binding entries to the hardware filtering table.
DHCPv6 snooping option 18/37 status	Indicates whether Option 18 or 37 is added to DHCPv6 request packets.
DHCPv6 snooping link detection	Indicates whether dynamically bound entries on a linkdown interface are cleared.
Interface	Interface name
Trusted	Indicates whether an interface is a trusted port.
Filter DHCP	Indicates whether DHCPv6 request packet filtering is configured.

Notifications

N/A

Platform Description

N/A

1.17 show ipv6 dhcp snooping vlan

Function

Run the **show ipv6 dhcp snooping vlan** command to display VLANs to which DHCPv6 Snooping does not take effect.

Syntax

show ipv6 dhcp snooping vlan

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays VLANs to which DHCPv6 Snooping does not take effect.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping vlan
VLAN Name       Closed
2    VLAN 2     YES
```

Table 1-2 Output Fields of the show ipv6 dhcp snooping vlan Command

Field	Description
VLAN	VLAN ID.
Name	VLAN name.
Closed	Indicates whether DHCPv6 Snooping takes effect.

Notifications

N/A

Platform Description

N/A

1.18 show ipv6 dhcp snooping binding

Function

Run the **show ipv6 dhcp snooping binding** command to display dynamic user information in the DHCPv6 Snooping binding database.

Syntax

show ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address for which binding information is displayed.

mac-address: MAC address for which binding information is displayed.

vlan *vlan-id*: Specifies the VLAN for which binding information is displayed.

interface *interface-type interface-number*: Specifies the interface for which binding information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays dynamic user information in the DHCPv6 Snooping binding database.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping binding
Total number of bindings: 1
NO.   MAC Address        IPv6 Address                              Lease(sec)   VLAN
Interface
1     00d0.f801.0101     2001::10                                  42368        2
GigabitEthernet 0/1
```

Table 1-3 Output Fields of the show ipv6 dhcp snooping binding Command

Field	Description
Total number of bindings	Number of bindings in the DHCPv6 Snooping binding database
No.	Record number
MAC Address	MAC address of a user
IPv6 Address	IPv6 address of a user
Lease(sec)	Lease time of a record
VLAN	VLAN of a user
Interface	Wired access interface of a user

Notifications

N/A

Platform Description

N/A

1.19 show ipv6 dhcp snooping prefix

Function

Run the **show ipv6 dhcp snooping prefix** command to display user information in the DHCPv6 Snooping prefix database.

Syntax

show ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address for which user information is displayed.

mac-address: MAC address for which user information is displayed.

vlan *vlan-id*: Specifies the VLAN for which user information in the prefix database is displayed.

interface *interface-type interface-number*: Specifies the interface for which user information in the prefix database is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays user information in the DHCPv6 Snooping prefix database.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping prefix
Total number of bindings: 1
NO.   MAC Address        IPv6 Address                       Lease(sec)   VLAN
Interface
1     00d0.f801.0101     2001:2002::/64                      42368       2
GigabitEthernet 0/1
```

Table 1-4 Output Fields of the show ipv6 dhcp snooping prefix Command

Field	Description
Total number of bindings	Number of bindings in the DHCPv6 Snooping prefix database
No.	Record number
MAC Address	MAC address of a user
IPv6 Address	IPv6 address of a user
Lease(sec)	Lease time of a record
VLAN	VLAN of a user
Interface	Access interface of a user

Notifications

N/A

Platform Description

N/A

1.20 show ipv6 dhcp snooping statistics

Function

Run the **show ipv6 dhcp snooping statistics** command to display statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.

Syntax

show ipv6 dhcp snooping statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping statistics
Packets processed by DHCPv6 snooping = 0
Packets dropped because
Received on untrusted ports        = 0
Relay forward                    = 0
No binding entry                  = 0
Binding fail                     = 0
Unknown packet                    = 0
Unknown output interface           = 0
No enough memory                  = 0
Admin filter DCHPv6 packet         = 0
```

Table 1-5 Output Fields of the show ipv6 dhcp snooping statistics Command

Field	Description
Received on untrusted ports	Server response packets discarded on untrusted ports.
Relay forward	Discarded packets that are relayed once.
No binding entry	When the binding entry of a RELEASE or DECLINE packet does not exist or is incorrect, the packet is discarded.
Binding fail	Packets discarded because entry binding fails. Generally, entry binding fails because hardware resources are insufficient.
Unknown packet	Unknown DHCPv6 packets.
Unknown output interface	Packets sent from unknown outbound interface because the MAC address cannot be found or the interface is not set as a trusted port.
No enough memory	Packets discarded due to insufficient memory resources.
Admin filter-dhcpv6-pkt	DHCPv6 packets filtered due to the administrator configuration, mainly packets filtered after the **ipv6 dhcp snooping filter-dhcp-pkt** command is configured.

Notifications

N/A

Platform Description

N/A

1.21 show ipv6 dhcp snooping packet

Function

Run the **show ipv6 dhcp snooping packet** command to display statistics about packets related to the DHCPv6 Snooping function.

Syntax

show ipv6 dhcp snooping packet

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics about packets related to the DHCPv6 Snooping function.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping packet
Total port num:3 (port which process none packet doesn't display)
Interface    Total Recv  Total Drop   Total Fwd   SOLICIT(Drop/Fwd)
ADVERTISE(Drop/Fwd)     REQUEST(Drop/Fwd)       REPLY(Drop/Fwd)
---- ---------------------------------------------None
Gi0/1               1          0          1          0/1                  0/0
0/0                  0/0
Gi0/17              2          0          2          0/2                  0/0
0/0                  0/0
Lc0                 1          0          1          0/0                  0/1
0/0                  0/0
```

Table 1-6 Output Fields of the show ipv6 dhcp snooping packet Command

Field	Description
Total port num	Number of interfaces with DHCPv6 Snooping packet records
Interface	Interface name
Total Recv	Total number of received packets from the specified interface
Total Drop	Total number of discarded packets from the specified interface
Total Fwd	Total number of forwarded packets from the specified interface
SOLICIT (Drop/Fwd)	Total number of discarded and forwarded SOLICIT packets from the specified interface
ADVERTISE (Drop/Fwd)	Total number of discarded and forwarded ADVERTISE packets from the specified interface
REQUEST (Drop/Fwd)	Total number of discarded and forwarded REQUEST packets from the specified interface
REPLY (Drop/Fwd)	Total number of discarded and forwarded REPLY packets from the specified interface

Notifications

N/A

Platform Description

N/A

1 ND Snooping Commands

Command	Function
clear ipv6 nd snooping prefix	Clear IPv6 prefixes snooped in a virtual local area network (VLAN).
clear ipv6 nd snooping binding	Clear snooped Stateless Address Autoconfiguration (SLACC) users.
clear ipv6 nd snooping packet	Clear Neighbor Discovery (ND) Snooping packet statistics on an interface.
ipv6 nd snooping bind lifetime	Configure the lease of an ND Snooping binding entry.
ipv6 nd snooping bind limit	Configure the capacity for ND Snooping binding entries.
ipv6 nd snooping bind warning-threshold	Configure a capacity alarm threshold for the ND Snooping binding entries.
ipv6 nd snooping check address-resolution	Enable ND guard against address spoofing attacks.
ipv6 nd snooping detect packet	Configure the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.
ipv6 nd snooping detect wait	Configure the waiting time for a detection packet response.
ipv6 nd snooping enable	Enable the ND Snooping function to snoop the SLACC process.
ipv6 nd snooping enable vlan	Enable ND Snooping on a VLAN.
ipv6 nd snooping log enable	Enable the function of logging ND Snooping key information.
ipv6 nd snooping log limit	Configure the capacity for ND Snooping key information logs.
ipv6 nd snooping nd-check only	Configure ND Snooping to work only in ND packet validity check mode but not generate binding entries.
ipv6 nd snooping prefix vlan	Configure the prefix for static IPv6 addresses.
ipv6 nd snooping syslog enable	Enable the function of prompting ND Snooping key information.

ipv6 nd snooping syslog frequency	Configure the frequency of ND Snooping key information prompts.
ipv6 nd snooping tentative wait	Configure the waiting time for an address conflict response.
ipv6 nd snooping trust	Configure an interface as an ND Snooping trusted interface.
show ipv6 nd snooping prefix	Display snooped prefixes.
show ipv6 nd snooping binding	Display snooped ND Snooping binding entries.
show ipv6 nd snooping log	Display ND Snooping key information logs recorded in the memory.
show ipv6 nd snooping packet	Display ND Snooping packet statistics on an interface.

1.1 clear ipv6 nd snooping prefix

Function

Run the **clear ipv6 nd snooping prefix** command to clear IPv6 prefixes snooped in a virtual local area network (VLAN).

Syntax

clear ipv6 nd snooping prefix [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies the VLAN in which the snooped IPv6 prefixes are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears IPv6 prefixes snooped in all VLANs.

```
Hostname> enable
Hostname# clear ipv6 nd snooping prefix
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 nd snooping binding

Function

Run the **clear ipv6 nd snooping binding** command to clear snooped Stateless Address Autoconfiguration (SLACC) users.

Syntax

clear ipv6 nd snooping binding [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies the VLAN in which snooped SLACC users are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears SLACC users snooped in all VLANs.

```
Hostname> enable
Hostname# clear ipv6 nd snooping binding
```

Notifications

N/A

Platform Description

N/A

1.3 clear ipv6 nd snooping packet

Function

Run the **clear ipv6 nd snooping packet** command to clear Neighbor Discovery (ND) Snooping packet statistics on an interface.

Syntax

clear ipv6 nd snooping packet [**interface** *interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface on which the ND Snooping packet statistics are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear ND Snooping packet statistics on an interface, including the numbers of received, discarded, and forwarded ND packets, the total number of each type of ND packets, and the number of each type of ND packets discarded.

Examples

The following example clears ND Snooping packet statistics on all interfaces.

```
Hostname> enable
Hostname# clear ipv6 nd snooping packet
```

Notifications

N/A

Platform Description

N/A

1.4 ipv6 nd snooping bind lifetime

Function

Run the **ipv6 nd snooping bind lifetime** command to configure the lease of an ND Snooping binding entry.

Run the **no** form of this command to remove this configuration.

The lease time of an ND Snooping binding entry is 300s by default.

Syntax

ipv6 nd snooping bind lifetime *time*

no ipv6 nd snooping bind lifetime

Parameter Description

time: Lease time of an entry, in seconds. The range is from 5 to 604800.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the lease time for an entry to prevent binding entries from occupying the memory space for a long time.

Examples

The following example sets the lease time of an ND Snooping binding entry to 3600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind lifetime 3600
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.5 ipv6 nd snooping bind limit

Function

Run the **ipv6 nd snooping bind limit** command to configure the capacity for ND Snooping binding entries.

Run the **no** form of this command to remove this configuration.

The capacity for binding entries depends on the actual product by default.

Syntax

ipv6 nd snooping bind limit *limit*

no ipv6 nd snooping bind limit

Parameter Description

limit: Capacity for binding entry. The value range is from 7 to 1048576.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the capacity for binding entries. The configured value cannot be less than the current number of binding entries.

Examples

The following example sets the total capacity for binding entries to **1024** and sets that on GigabitEthernet 0/1 to **128**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind limit 1024
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping bind limit 128
Hostname(config-if-GigabitEthernet 0/1)# exit
```

Notifications

When the configured capacity value is smaller than the current number of binding entries, the following notification will be displayed:

```
% Failed to execute command, because of "current num more than config maximum".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping bind warning-threshold**

1.6 ipv6 nd snooping bind warning-threshold

Function

Run the **ipv6 nd snooping bind warning-threshold** command to configure a capacity alarm threshold for the ND Snooping binding entries.

Run the **no** form of this command to remove this configuration.

No capacity alarm threshold is configured for the ND Snooping binding entries by default.

Syntax

ipv6 nd snooping bind warning-threshold *number*

no ipv6 nd snooping bind warning-threshold

Parameter Description

number: Capacity alarm threshold for the binding entries, in percentage (%). The range is from 15 to 100.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a capacity alarm threshold for the binding entries. For example, if *num* is set to **60**, an alarm is triggered when the current number of entries exceeds 60% of the configured capacity and a prompt is displayed when the current number of entries is less than 60% of the configured capacity. When the configuration is canceled, *num* is set to **0**. In this case, no capacity alarm is triggered. When this command is configured on an interface and the capacity for binding entries is not limited on the interface (that is, the *limit* parameter in **ipv6 nd snooping bind limit** is set to **0**), no capacity alarm is triggered.

Examples

The following example sets the capacity alarm threshold for the global binding entries to **60** and sets that on GigabitEthernet 0/1 to **60**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind warning-threshold 60
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping bind warning-threshold 60
```

Notifications

When a capacity alarm threshold (for example, 15) is configured for the binding entries and the percentage of the current number of entries to the configured capacity exceeds the configured threshold, the following notification will be displayed:

```
The binding user has exceeded the 15 percent capacity of count limit.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping bind limit**

1.7 ipv6 nd snooping check address-resolution

Function

Run the **ipv6 nd snooping check address-resolution** command to enable ND guard against address spoofing attacks.

Run the **no** form of this command to disable this feature.

ND guard against address spoofing attacks is disabled by default.

Syntax

ipv6 nd snooping check address-resolution

no ipv6 nd snooping check address-resolution

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When ND guard against address spoofing attacks is enabled, the IPv6 address and Media Access Control (MAC) address fields in neighbor solicitation (NS), neighbor advertisement (NA), and router solicitation (RS) packets received on an interface are checked whether match the binding entries. ND packets that do not match the binding entries are discarded.

Note

The entries for ND guard against address spoofing attacks come from the Source Address Validation Improvements (SAVI) binding table instead of the ND Snooping binding table.

Examples

The following example enables ND guard against address spoofing attacks.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping check address-resolution
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ipv6 nd snooping detect packet

Function

Run the **ipv6 nd snooping detect packet** command to configure the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.

Run the **no** form of this command to remove this configuration.

Two detection packets are sent at an interval of 250 ms by default.

Syntax

ipv6 nd snooping detect packet *number* **interval** *time*

no ipv6 nd snooping detect packet

Parameter Description

number: Number of detection packets to be sent. The range is from 1 to 10.

time: Interval for sending detection packets, in milliseconds. The range is from 50 to 5000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device with ND Snooping enabled receives an NS or NA packet with an address that conflicts with that in a binding entry or the lease of a binding entry expires, the device sends a detection packet to the port recorded in the binding entry. This command is used to set the number of detection packets to be sent and the interval for sending detection packets.

Caution

The interval is only a reference value in ND Snooping for sending packets and may be inaccurate.

Examples

The following example sets the number of detection packets to be sent to **2** and the interval for sending detection packets to **2000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping detect packet 2 interval 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping log limit**

1.9 ipv6 nd snooping detect wait

Function

Run the **ipv6 nd snooping detect wait** command to configure the waiting time for a detection packet response.

Run the **no** form of this command to remove this configuration.

The default waiting time for a detection packet response is 500 ms.

Syntax

ipv6 nd snooping detect wait *time*

no ipv6 nd snooping detect wait

Parameter Description

time: Waiting time, in milliseconds. The range is from 50 to 5000. The waiting time is only a reference value in ND Snooping and may be inaccurate.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the waiting time for a detection packet response after the device with ND Snooping enabled sends a detection packet. If no response is received within the waiting time, the device deletes the corresponding entry.

Examples

The following example sets the waiting time for a detection packet response to 2000 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping detect wait 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping detect packet**

1.10 ipv6 nd snooping enable

Function

Run the **ipv6 nd snooping enable** command to enable the ND Snooping function to snoop the SLACC process.

Run the **no** form of this command to disable this feature.

ND Snooping is disabled by default.

Syntax

ipv6 nd snooping enable

no ipv6 nd snooping enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Snooped SLACC user information can be used for ND guard and other security policies.

Examples

The following example enables ND Snooping.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 nd snooping enable vlan

Function

Run the **ipv6 nd snooping enable vlan** command to enable ND Snooping on a VLAN.

Run the **no** form of this command to remove this feature.

After ND Snooping is enabled on a device, it takes effect to all VLANs of the device by default.

Syntax

ipv6 nd snooping enable vlan { *vlan-range* | *vlan-id* }

no ipv6 nd snooping enable vlan { *vlan-range* | *vlan-id* }

Parameter Description

vlan-range: Range of VLANs to which ND Snooping takes effect. The value is a character string, for example 1, 3–5, 7, and 9–11.

vlan-id: ID of a VLAN. The range is from 1 to 4096.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If SLACC snooping is not required in a VLAN, you can run this command to disable ND Snooping on the VLAN.

Examples

The following example disables ND Snooping on VLAN 5 and VLANs 10 to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
Hostname(config)# no ipv6 nd snooping enable vlan 5,10-20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ipv6 nd snooping log enable

Function

Run the **ipv6 nd snooping log enable** command to enable the function of logging ND Snooping key information.

Run the **no** form of this command to disable this feature and clear key information logs in the memory.

The function of logging ND Snooping key information is disabled by default.

Syntax

ipv6 nd snooping log enable

no ipv6 nd snooping log enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After enabling ND guard against address spoofing attacks or RA attacks, you can run this command to enable the function of logging ND Snooping key information. When the device receives packets for address spoofing attacks or RA attacks, information about the attacker is recorded to the memory via attack logs.

Examples

The following example enables the function of logging ND Snooping key information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping log enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping log limit**

1.13 ipv6 nd snooping log limit

Function

Run the **ipv6 nd snooping log limit** command to configure the capacity for ND Snooping key information logs.

Run the **no** form of this command to remove this configuration.

A maximum of 1000 ND Snooping key information logs can be recorded by default.

Syntax

ipv6 nd snooping log limit *number*

no ipv6 nd snooping log limit *number*

Parameter Description

number: Capacity value. The value range is from 50 to 5000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the capacity for address spoofing or RA attack logs reaches the upper limit, new attack logs replace the earliest ones.

Examples

The following example sets the capacity for ND Snooping key information logs to **500**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping log limit 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping log enable**

1.14 ipv6 nd snooping nd-check only

Function

Run the **ipv6 nd snooping nd-check only** command to configure ND Snooping to work only in ND packet validity check mode but not generate binding entries.

Run the **no** form of this command to remove this configuration.

ND Snooping is not configured to work only in ND packet validity check mode by default.

Syntax

ipv6 nd snooping nd-check only

no ipv6 nd snooping nd-check only

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be configured when ND Snooping entries do not need to be generated but the ND packet validity needs to be checked.

Note

This command takes effect only after ND Snooping is enabled.

Examples

The following example configures ND Snooping to work only in ND packet validity check mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
Hostname(config)# ipv6 nd snooping nd-check only
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.15 ipv6 nd snooping prefix vlan

Function

Run the **ipv6 nd snooping prefix vlan** command to configure the prefix for static IPv6 addresses.

Run the **no** form of this command to remove this configuration.

No prefix is configured for static IPv6 addresses by default.

Syntax

ipv6 nd snooping prefix vlan *vlan-id ipv6-address/prefix-length*

no ipv6 nd snooping prefix vlan *vlan-id ipv6-address/prefix-length*

Parameter Description

vlan-id: Access VLAN.

ipv6-address/prefix-length-address/prefix-length: IPv6 address and prefix.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to configure IPv6 address prefix entries.

Examples

The following example sets the prefix for ND Snooping static IPv6 addresses to 2018:7::/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping prefix vlan 1 2018:7::/64
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ipv6 nd snooping syslog enable

Function

Run the **ipv6 nd snooping syslog enable** command to enable the function of prompting ND Snooping key information.

Run the **no** form of this command to disable this feature.

The function of prompting ND Snooping key information is disabled by default.

Syntax

ipv6 nd snooping syslog enable

no ipv6 nd snooping syslog enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After enabling ND guard against address spoofing attacks or RA attacks, you can run this command to enable the function of prompting ND Snooping key information. When the device receives packets of address spoofing attacks or RA attacks, information about the attacker is displayed via system prompts.

Examples

The following example enables the function of prompting ND Snooping key information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping syslog enable
```

Notifications

```
*Dec 27 20:34:13: %ND_SNP-COLLISION: Receive Address Resolution attack from
host<VLAN=2,port=Gi0/16,MAC=e0db.5594.c026,IPv6=fe80::11da:cb7e:57db:e231> was
detected.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping syslog frequency**

1.17 ipv6 nd snooping syslog frequency

Function

Run the **ipv6 nd snooping syslog frequency** command to configure the frequency of ND Snooping key information prompts.

Run the **no** form of this command to remove this configuration.

A maximum of 5 prompts for ND Snooping key information are provided every second by default.

Syntax

ipv6 nd snooping syslog frequency *number*

no ipv6 nd snooping syslog frequency

Parameter Description

number: Frequency of system prompts, in pieces per second. The range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the frequency of ND Snooping key information prompts, that is, the maximum number of system prompts generated every second. When key information is generated, such as information about address spoofing attacks, RA attacks, capacity threshold alarms, and entry capacity alarms, the system generates corresponding prompt logs. When the number of logs generated every second is greater than the configured frequency, the system displays logs within the frequency range only and discard remaining logs to prevent the screen from frequent refreshing.

Caution

The log limit function is implemented based on the system time, while the log display is implemented based on the user time. Therefore, the number of logs with the same time on the console is [0, 2 x *num*].

Examples

The following example sets the frequency of ND Snooping key information prompts to 200 pieces per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping syslog frequency 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 nd snooping syslog enable**

1.18 ipv6 nd snooping tentative wait

Function

Run the **ipv6 nd snooping tentative wait** command to configure the waiting time for an address conflict response.

Run the **no** form of this command to remove this configuration.

The default waiting time for an address conflict response is 500 ms.

Syntax

ipv6 nd snooping tentative wait *time*

no ipv6 nd snooping tentative wait

Parameter Description

time: Waiting time, in milliseconds. The range is from 50 to 5000. The waiting time is only a reference value in ND Snooping and may be inaccurate.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device with ND Snooping enabled receives a DAD_NS packet (for duplicate address check) from a client, the device creates an entry in **TENTATIVE** state. The entry is changed to a formal binding entry after a period of time.

Examples

The following example sets the waiting time for an address conflict response to 2000 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping tentative wait 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ipv6 nd snooping trust

Function

Run the **ipv6 nd snooping trust** command to configure an interface as an ND Snooping trusted interface.

Run the **no** form of this command to remove this configuration.

All interfaces are ND Snooping untrusted interfaces by default.

Syntax

ipv6 nd snooping trust

no ipv6 nd snooping trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After an interface is configured as an ND Snooping trusted interface, RA and RR packets received on this interface are forwarded, and such packets received on untrusted interfaces are discarded.

This command can be configured only on L2 switching ports, aggregation ports (APs), or encapsulation sub-interfaces.

Note

Generally, uplink interfaces, that is, interfaces connected to trusted gateways are configured as trusted interfaces.

Examples

The following example configures GigabitEthernet 0/1 as an ND Snooping trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ipv6 nd snooping prefix

Function

Run the **show ipv6 nd snooping prefix** command to display snooped prefixes.

Syntax

show ipv6 nd snooping prefix

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays snooped prefixes.

```
Hostname> enable
Hostname# show ipv6 nd snooping prefix
VLAN  Prefix                              Lifetime(s)
----  ------                              -----------
2     1001::/64                           STATIC
```

Table 1-1 Output Fields of the show ipv6 nd snooping prefix Command

Field	Description
Prefix	Prefix
lifetime	Lease

Notifications

N/A

Platform Description

N/A

1.21 show ipv6 nd snooping binding

Function

Run the **show ipv6 nd snooping binding** command to display snooped ND Snooping binding entries.

Syntax

show ipv6 nd snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address with its binding entry displayed.

mac-address: MAC address with its binding entry displayed.

vlan-id: VLAN with learned binding entries displayed.

interface-type interface-number: Interface with learned binding entries displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays snooped ND Snooping binding entries.

```
Hostname> enable
Hostname# show ipv6 nd snooping binding
Total number of bindings: 5
VLAN MAC address     Interface   State        IPv6 address
Life time(s)
1024 b8ac.6fc8.8b9a   Gi3/17      VALID        2018:5::1
14376
1024 b8ac.6fc8.8b9a   Gi3/17      TENTATIVE    2018:5::48ed:679a:a862:febd
5
1024 b8ac.6fc8.8b9a   Gi3/17      VALID        2018:5::8880:86f0:ebda:c734
14381
1024 b8ac.6fc8.8b9a   Gi3/17      VALID        2018:5::c58f:91d1:3dab:4e85
14381
1024 b8ac.6fc8.8b9a   Gi3/17      VALID        fe80::c58f:91d1:3dab:4e85
14376
```

Table 1-2 Output Fields of the show ipv6 nd snooping binding Command

Field	Description
MAC address	MAC address
Interface	Interface
State	Status
IPv6 address	IPv6 address
Life time	Lease

Notifications

N/A

Platform Description

N/A

1.22 show ipv6 nd snooping log

Function

Run the **show ipv6 nd snooping log** command to display ND Snooping key information logs recorded in the memory.

Syntax

show ipv6 nd snooping log

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays ND Snooping key information logs recorded in the memory.

```
Hostname> enable
Hostname# show ipv6 nd snooping log
Total log num:3
Time              Event        Packet                          IPv6 Address
MAC VLAN   PORT
2017-12-27 20:34:15 ND Error        NA              fe80::11da:cb7e:57db:e231
e0db.5594.c026   2  Gi0/16
2017-12-27 20:34:14 ND Error        NA              fe80::11da:cb7e:57db:e231
e0db.5594.c026   2  Gi0/16
2017-12-27 20:34:13 ND Error        NA              fe80::11da:cb7e:57db:e231
e0db.5594.c026   2  Gi0/16
```

Table 1-3 Output Fields of the show ipv6 nd snooping log Command

Field	Description
Time	Time when an address spoofing attack packet or RA attack packet is received
Event	Type of an attack packet
Packet	Content of an attack packet

IPv6 address	IPv6 address used by an attacker
MAC	MAC address used by an attacker
VLAN	ID of the source VLAN of an attack packet
PORT	ID of the source port of an attack packet

Notifications

N/A

Platform Description

N/A

1.23 show ipv6 nd snooping packet

Function

Run the **show ipv6 nd snooping packet** command to display ND Snooping packet statistics on an interface.

Syntax

show ipv6 nd snooping packet

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays ND Snooping packet statistics on an interface.

```
Hostname> enable
Hostname# show ipv6 nd snooping packet
Total port num:145 (port which process none packet doesn't display)
Interface    Total Recv  Total Drop   Total Fwd  NS Discard/ NS Process  NA Discard/
NA Process  RS Discard/ RS Process  RA Discard/ RA Process  RR Discard/ RR Process
Gi7/1            11863      10883        980         0/        70          0/
875          0/        35      10883/     10883          0/         0
Lc0               189          0        189          0/        70          0/
70          0/         0          0/        49          0/         0
```

Table 1-4 Output Fields of the show ipv6 nd snooping packet Command

Field	Description
Interface	Interface name
Total Recv	Total number of packets received on the interface
Total Drop	Total number of discarded packets from the specified interface
Total Fwd	Total number of forwarded packets from the specified interface
NS Discard	Total number of discarded NS packets from the interface
NS Process	Total number of NS packets from the interface processed by ND Snooping
NA Discard	Total number of discarded NA packets from the interface
NA Process	Total number of NA packets from the interface processed by ND Snooping
RS Discard	Total number of discarded RS packets from the interface
RS Process	Total number of RS packets from the interface processed by ND Snooping
RA Discard	Total number of discarded RA packets from the interface
RA Process	Total number of RA packets from the interface processed by ND Snooping
RR Discard	Total number of discarded RR packets from the interface
RR Process	Total number of RR packets from the interface processed by ND Snooping

Notifications

N/A

Platform Description

N/A

1 TCP Commands

Command	Function
ip tcp keepalive	Enable the TCP keepalive function.
ip tcp mss	Configure the upper MSS limit for a TCP connection.
ip tcp path-mtu-discovery	Enable the path MTU discovery function of TCP.
ip tcp send-reset	Configure the sending of TCP reset packets upon the receiving of port unreachable messages.
ip tcp synwait-time	Configure the timeout period of SYN packets used for connection establishment.
ip tcp window-size	Configure the TCP window size.
show ipv6 tcp connect	Display the basic information about the current IPv6 TCP connection.
show ipv6 tcp connect statistics	Display the statistics on all the current IPv6 TCP connections.
show ipv6 tcp pmtu	Display the path MTU of an IPv6 TCP connection.
show ipv6 tcp port	Display the usage of the current IPv6 TCP port.
show tcp connect	Display the basic information about the current IPv4 TCP connection.
show tcp connect statistics	Display the statistics on all the current IPv4 TCP connections.
show tcp parameter	Display the information about current TCP parameters.
show tcp pmtu	Display the path MTU of an IPv4 TCP connection.
show tcp port	Display the usage of the current IPv4 TCP port.
show tcp statistics	Display the current TCP statistics of the system.

1.1 ip tcp keepalive

Function

Run the **ip tcp keepalive** command to enable the TCP keepalive function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The TCP keepalive function is disabled by default.

Syntax

ip tcp keepalive [**interval** *interval*] [**times** *times*] [**idle-period** *time*]

no ip tcp keepalive

default ip tcp keepalive

Parameter Description

interval *interval*: Indicates the interval time at which a keepalive packet is transmitted, in seconds. The value range is from 1 to 120. The default value is **75**.

times *times*: Indicates the keepalive packet transmission count. The value range is from 1 to 10, and the default value is **6**.

idle-period *time*: Indicates the idle period, in seconds, that is, the length of time that the peer end does not send a packet to the local end. The value range is from 60 to 1800. The default value is **900**, that is, 15 minutes.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

You may enable the keepalive function to check whether the peer end of a TCP connection works normally.

Suppose that the TCP keepalive function is enabled on a device and default interval, transmission count, and idle period settings are used. If no packet is received from the peer within 15 minutes, the device starts sending keepalive packets every 75 seconds for 6 consecutive times. If the device receives no TCP packet from the peer, it considers the TCP connection invalid and automatically releases the TCP connection.

This command is no different to the server and client and applies to all TCP connections.

Examples

The following example enables the TCP keepalive function on a device with the idle period, interval, and transmission count set to 3 minutes, 60 seconds, and 4 respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

This command has superseded the **service tcp-keepalives-in** and **service tcp-keepalives-out** commands.

Related Commands

N/A

1.2 ip tcp mss

Function

Run the **ip tcp mss** command to configure the upper MSS limit for a TCP connection.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The calculated value "IPv4/IPv6 MTU – IPv4/IPv6 header length – TCP header length" is used as the upper MSS limit by default.

Syntax

ip tcp mss *max-segment-size*

no ip tcp mss

default ip tcp mss

Parameter Description

max-segment-size: Upper MSS limit. The value range is from 68 to 10000, in bytes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The MSS refers to the maximum length of data payload in a TCP segment, excluding the TCP option.

This command is used to restrict the MSS limit for TCP connections to be established. The negotiated MSS for a new connection should be smaller than this MSS.

This parameter does not need to be configured by default. Instead, the MSS calculated based on the MTU is used, as shown below:

IPv4 TCP: MSS = IP MTU of the outbound interface corresponding to the peer IP address – IP header size (20 bytes) – TCP header size (20 bytes).

IPv6 TCP: MSS = Path MTU corresponding to the peer IPv6 address – IPv6 header size (40 bytes) – TCP header size (20 bytes).

If a connection supports certain options, the option length after 4-byte alignment should be deducted from the MSS value. For example, 20 bytes need to be deducted if the MD5 option is used because the length of the MD5 option is 18 bytes and the length after alignment is 20 bytes.

If an upper MSS limit is configured, the upper MSS limit that actually takes effect is the MSS calculated based on the MTU or configured MSS, whichever is smaller.

Examples

The following example sets the upper MSS limit of TCP connections to 1,300 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp mss 1300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip tcp path-mtu-discovery

Function

Run the **ip tcp path-mtu-discovery** command to enable the path MTU discovery function of TCP.

Run the **no** form of this command to disable this feature.

The path MTU discovery function of TCP is disabled by default.

Syntax

ip tcp path-mtu-discovery [**age-timer** *time* | **age-timer infinite**]

no ip tcp path-mtu-discovery

Parameter Description

age-timer *time*: Indicates the interval for a new probe after TCP discovers a path MTU, in minutes. The value range is from 10 to 30. The default value is **10**.

age-timer infinite: Indicates that no probe is performed after TCP discovers a path MTU.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The path MTU discovery function of TCP is implemented according to RFC1191 to improve the network bandwidth utilization. When TCP is applied to bulk transmit chunk data, this function can improve transmission performance greatly.

After discovering the path MTU, TCP can use a larger MSS to probe a new path MTU at intervals. This interval is specified by using the **age-timer** parameter. When the device discovers a path MTU smaller than the MSS negotiated by both ends of a TCP connection, the device tries to probe a larger path MTU at the configured interval described above. The probe process is stopped when the path MTU reaches the MSS or the user turns off the timer. You may use the **age-timer infinite** parameter to turn off this timer.

This command applies to only IPv4 TCP. The path MTU discovery function of IPv6 TCP is enabled permanently and cannot be disabled.

Examples

The following example enables the path MTU discovery function of TCP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp path-mtu-discovery
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip tcp send-reset

Function

Run the **ip tcp send-reset** command to configure the sending of TCP reset packets upon the receiving of port unreachable messages.

Run the **no** form of this command to remove this configuration.

TCP reset packets are sent upon the receiving of port unreachable messages by default.

Syntax

ip tcp send-reset

no ip tcp send-reset

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In general, when the TCP module distributes a TCP packet, if the TCP connection, to which the packet belongs, cannot be identified, the local end sends a reset packet to the peer end to terminate the TCP connection. This, however, can also become a target for attackers. A large number of TCP port unreachable messages can impose attacks on the device. You can use this command to prevent the sending of TCP reset packets upon the receiving of port unreachable messages.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example configures the device not to send TCP reset packets upon the receiving of port unreachable messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip tcp send-reset
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip tcp synwait-time

Function

Run the **ip tcp synwait-time** command to configure the timeout period of SYN packets used for connection establishment.

Run the **no** form of this command to restore the default configuration.

The default timeout period of SYN packets used for connection establishment is 20 seconds.

Syntax

ip tcp synwait-time *time*

no ip tcp synwait-time

Parameter Description

time: SYN packet timeout period, in seconds. The value range is from 5 to 300. The default value is **20**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In case of SYN flooding, shortening SYN timeout period can reduce resource consumption. However, it does not work on continuous SYN flooding.

When a device actively requests to establish a connection with an external device, shortening SYN timeout period can reduces users' waiting time, for example, waiting time in the telnet connection. You may prolong SYN timeout period properly for a poor network.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example sets the timeout period of SYN packets used for connection establishment to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp synwait-time 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip tcp window-size

Function

Run the **ip tcp window-size** command to configure the TCP window size.

Run the **no** form of this command to restore the default configuration.

The default TCP window size is 65,535 bytes.

Syntax

ip tcp window-size *size*

no ip tcp window-size

Parameter Description

size: Window size, in bytes. The value range is from 128 to 1073725440.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The TCP receive buffer is used to buffer data from the peer. The data will be subsequently read by applications. The TCP window size reflects the size of idle space in the receive buffer. For bulk-data connections, enlarging the window size dramatically promotes TCP transmission performance.

If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example sets the TCP window size to 16,386 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp window-size 16386
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show ipv6 tcp connect

Function

Run the **show ipv6 tcp connect** command to display the basic information about the current IPv6 TCP connection.

Syntax

show ipv6 tcp connect [**local-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-ipv6** *ipv6-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]

Parameter Description

local-ipv6 *ipv6-address*: Indicates a local IPv6 address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ipv6 *ipv6-address*: Indicates a peer IPv6 address. The value range is from 1 to 65535.

peer-port *port-number*: Indicates a peer port.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the basic information about all IPv6 TCP connections is displayed.

Examples

The following example displays the basic information about the current IPv6 TCP connections.

```
Hostname> enable
Hostname# show ipv6 tcp connect
Number Local Address    Foreign Address        State       Process name
1     :::22           :::0                LISTEN      rg-sshd
2     :::23           :::0                LISTEN      rg-telnetd
3     1000::1:23       1000::2:64201          ESTABLISHED  rg-telnetd
```

The following example displays the basic information about the current IPv6 TCP connection in VRF-IPv6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf-ipv6
Hostname(config-vrf)# address-family ipv6
Hostname(config-vrf-af)# show ipv6 tcp connect vrf-name vrf-ipv6
Number   Local Address   Foreign Address       STATE        Process name     VRF name
1       :::23          :::0                LISTEN       telnetd-main     vrf-ipv6
```

Table 1-1 Output Fields of the show ipv6 tcp connect Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the last colon is the port number.

Field	Description
Foreign Address	Remote address and port number. The number after the last colon is the port number.
State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.8 show ipv6 tcp connect statistics

Function

Run the **show ipv6 tcp connect statistics** command to display the statistics on all the current IPv6 TCP connections.

Syntax

show ipv6 tcp connect statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the statistics on all the current IPv6 TCP connections.

```
Hostname# show ipv6 tcp connect statistics

State              Count
-----              -----
ESTABLISHED         1
SYN_SENT           0
SYN_RECV           0
FIN_WAIT1          0
FIN_WAIT2          0
TIME_WAIT          0
CLOSED             0
CLOSE_WAIT         0
LAST_ACK           0
LISTEN             15
CLOSING            0
NEW_SYN_RECV        0
Total: 16
```

Table 1-2 Output Fields of the show ipv6 tcp connect statistics Command

Field	Description

Field	Description
State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Count	Number of times that connections are in a specific state.
Total	Total count.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show ipv6 tcp pmtu

Function

Run the **show ipv6 tcp pmtu** command to display the path MTU of an IPv6 TCP connection.

Syntax

show ipv6 tcp pmtu [**local-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-ipv6** *ipv6-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]

Parameter Description

local-ipv6 *ipv6-address*: Indicates a local IPv6 address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ipv6 *ipv6-address*: Indicates a peer IPv6 address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the path MTUs of all IPv6 TCP connections are displayed.

Examples

The following example displays the path MTUs of IPv6 TCP connections.

```
Hostname> enable
Hostname# show ipv6 tcp pmtu
Number  Local Address          Foreign Address       PMTU
1      1000::1:23            1000::2.13560        1440
```

Table 1-3 Output Fields of the show ipv6 tcp pmtu Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
PMTU	Path MTU.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.10 show ipv6 tcp port

Function

Run the **show ipv6 tcp port** command to display the usage of the current IPv6 TCP port.

Syntax

show ipv6 tcp port [*port-number*]

Parameter Description

port-number: Specified port number. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the usage of all current IPv6 TCP ports is displayed.

Examples

The following example displays the usage of the current IPv6 TCP ports.

```
Hostname> enable
Hostname# show ipv6 tcp port
TCP connections on port 23:
Number  Local Address Foreign Address   State
1      1000::1:23   1000::2:64571     ESTABLISHED
Total: 1
TCP connections on port 2650:
Number  Local Address Foreign Address   State
Total: 0
```

Table 1-4 Output Fields of the show ipv6 tcp port Command

Field	Description
Number	Serial number.
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

Field	Description
State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Total	Total number of information entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show tcp connect

Function

Run the **show tcp connect** command to display the basic information about the current IPv4 TCP connection.

Syntax

show tcp connect [**local-ip** *ip-address*] [**local-port** *port-number*] [**peer-ip** *ip-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]

Parameter Description

local-ip *ip-address*: Indicates a local IP address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ip *ip-address*: Indicates a peer IP address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is not configured, the basic information about all IPv4 TCP connections is displayed.

Examples

The following example displays the basic information about the current IPv4 TCP connections.

```
Hostname> enable
Hostname# show tcp connect
Number Local Address    Foreign Address         State      Process name
1      0.0.0.0:22       0.0.0.0:0              LISTEN     rg-sshd
2      0.0.0.0:23       0.0.0.0:0              LISTEN     rg-telnetd
3      1.1.1.1:23       1.1.1.2:64201           ESTABLISHED rg-telnetd
```

Table 1-5 Output Fields of the show tcp connect Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the colon is the port number, for example, "23" in "1.1.1.1:23" is a port number.
Foreign Address	Remote address and port number. The number after the colon is the port number, for example, "23" in "1.1.1.1:23" is a port number.

Field	Description
State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.12 show tcp connect statistics

Function

Run the **show tcp connect statistics** command to display the statistics on all the current IPv4 TCP connections.

Syntax

show tcp connect statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the statistics on all the current IPv4 TCP connection.

```
Hostname> enable
Hostname# show tcp connect statistics
State              Count
-----              -----
ESTABLISHED         23
SYN_SENT           36
SYN_RECV           0
FIN_WAIT1          0
FIN_WAIT2          0
TIME_WAIT          0
CLOSED             0
CLOSE_WAIT         0
LAST_ACK           0
LISTEN             23
CLOSING            0
NEW_SYN_RECV        0
Total: 82
```

Table 1-6 Output Fields of the show tcp connect statistics Command

Field	Description
State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Count	Number of times that connections are in a specific state.
Total	Total count.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show tcp parameter

Function

Run the **show tcp parameter** command to display the information about current TCP parameters.

Syntax

show tcp parameter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the information about the current TCP parameters.

```
Hostname> enable
Hostname# show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit: bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
  Max SYN retries: 5
  Max SYN ACK retries: 5
Timewait specific information:
  Max timewait sockets: 180000
  Current timewait sockets: 0
  Timewait recycle: 0
  Reuse timewait port: 0
Keepalive information:
  Keepalive on: 0
  Idle period: 900 seconds
  Interval: 75 seconds
  Max probes: 6
MTU probing:
  Enable mtu probing: 0
FIN specific information:
  FIN_WAIT_2 timeout: 60 seconds
```

```
Orphan socket information:
  Max orphans: 16384
  Max orphan retries: 0
  Current orphans: 0
```

Table 1-7 Output Fields of the show tcp parameter Command

Field	Description
Hash table information	Hash table information of TCP connections.
Established hash bucket size	Hash bucket size of TCP connections in established status.
Bind hash bucket size	Hash bucket size of a listening port.
Memory information	Parameter information of Rx and Tx buffers of TCP connections.
Global memory limit	Global memory limit.
low=x	Memory limit of TCP sockets.
pressure=x	Memory alarm level of TCP sockets.
high=x (unit: pages)	Maximum memory usage of TCP sockets. The system will deny allocating sockets when the memory usage exceeds this value.
Per-socket receive buffer size	Size of the socket Rx buffer.
min=x	Minimum size of the socket buffer.
default=x	Default size of the socket buffer.
max=x (unit: bytes)	Maximum size of the socket buffer.
Per-socket send buffer size	Size of the socket Tx buffer.
Current allocated memory	Memory currently used by sockets.
Current memory pressure flag	Whether the current memory usage of sockets exceeds the alarm level.
SYN specific information	Parameter information related to connections and listening on the TCP server side.
Max SYN_RECV sockets per LISTEN socket	Maximum number of SYN connections of the listening socket.
Max SYN retries	Maximum retransmission count of SYN packets.
Max SYN ACK retries	Maximum retransmission count of SYN ACK packets.
Timewait specific information	Parameter information of TCP connections in TIME-WAIT status.
Max timewait sockets	Maximum number of TCP connections in TIME-WAIT status.
Current timewait sockets	Number of current TCP connections in TIME-WAIT status.
Timewait recycle	Quick reclamation of TCP connections in TIME-WAIT status.

Field	Description
Reuse timewait port	Port reuse of TCP connections in TIME-WAIT status.
Keepalive information	Parameter information of the TCP keepalive time.
Keepalive on	Whether the TCP keepalive function is enabled.
Idle period	Idle period of TCP keepalive.
Interval	TCP keepalive interval.
Max probes	TCP keepalive probing count.
MTU probing	Parameter information related to MTU probing.
Enable mtu probing	Whether MTU probing is enabled.
FIN specific information	Parameter information related to closing of TCP connections.
FIN_WAIT_2 timeout	Timeout period in FIN-WAIT-2 status.
Orphan socket information	Parameter information of TCP connections not associated with a specific application.
Max orphans	Maximum number of TCP connections not associated with a specific application.
Max orphan retries	Maximum retransmission count of TCP packets not associated with a specific application.
Current orphans	Number of current TCP connections not associated with a specific application.

Notifications

N/A

1.14 show tcp pmtu

Function

Run the **show tcp pmtu** command to display the path MTU of an IPv4 TCP connection.

Syntax

show tcp pmtu [**local-ip** *ip-address*] [**local-port** *port-number*] [**peer-ip** *ip-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]

Parameter Description

local-ip *ip-address*: Indicates a local IP address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ip *ip-address*: Indicates a peer IP address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the path MTUs of all IPv4 TCP connections are displayed.

Examples

The following example displays the path MTUs of IPv4 TCP connections.

```
Hostname> enable
Hostname# show tcp pmtu
Number  Local Address          Foreign Address       PMTU
1      192.168.195.212.23     192.168.195.112.13560  1440
```

Table 1-8 Output Fields of the show tcp pmtu Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the colon is the port number, for example, "23" in "192.168.195.212.23" is a port number.
Foreign Address	Remote address and port number. The number after the colon is the port number, for example, "23" in "192.168.195.212.23" is a port number.
PMTU	Path MTU.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.15 show tcp port

Function

Run the **show tcp port** command to display the usage of the current IPv4 TCP port.

Syntax

show tcp port [*port-number*]

Parameter Description

port-number: Specified port number. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the usage of all current IPv4 TCP ports is displayed.

Examples

The following example displays the usage of the current IPv4 TCP ports.

```
Hostname> enable
Hostname#show tcp port
TCP connections on port 23:
Number  Local Address Foreign Address    State
1      1.1.1.1:23    1.1.1.2:64571    ESTABLISHED
Total: 1
TCP connections on port 2650:
Number  Local Address Foreign Address    State
Total: 0
```

Table 1-9 Output Fields of the show tcp port Command

Field	Description
Number	Serial number.
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

State	Current status of a TCP connection: ● **CLOSED**: Indicates that the connection is closed. ● **LISTEN**: Indicates the listening status. ● **SYNSENT**: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● **SYNRCVD**: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● **ESTABLISHED**: Indicates that the connection is established. ● **FINWAIT1**: Indicates that the FIN packet has been sent from the local end. ● **FINWAIT2**: Indicates that the FIN packet sent from the local end has been acknowledged. ● **CLOSEWAIT**: Indicates that the local end has received the FIN packet from the peer end. ● **LASTACK**: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● **CLOSING**: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● **TIMEWAIT**: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● **NEW_SYN_RECV**: Indicates a new TCP connection request.
Total	Total number of information entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show tcp statistics

Function

Run the **show tcp statistics** command to display the current TCP statistics of the system.

Syntax

show tcp statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display the current TCP statistics of the system, including packet receiving information, three-way handshake information, and time-wait connection information.

Examples

The following example displays the current TCP statistics of the system.

```
Hostname> enable
Hostname#show tcp statistics
TCP Packets
  Received: 23243
  Errors  : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
  Accept backlog full: 0
  Web authentication limit per user: 0
  Failed to alloc memory for request sock: 0
  Failed to create open request child: 0
  SYN ACK retransmits: 0
  Timeouted requests: 0
  Web authentication:
    Limit per user: 0
    SYN ACK retransmission times-users: 0-0,1-0, 2-0,>=3-0
    Handshake fails: 0
Time-wait
  Time-wait bucket table overflow: 0
```

Table 1-10 Output Fields of the show tcp statistics Command

Field	Description
TCP Packets	Statistics on TCP packets received.
Received	Number of TCP packets received.
Errors	Number of TCP error packets received.
Three way handshake	Information about the three-way handshake process.
Request queue overflow	Number of packets discarded due to SYN queue overflow.
Accept backlog full	Number of packets discarded due to Accept queue overflow

Web authentication limit per user	Maximum concurrency of three-way handshake processes supported by a terminal to complete Web-based authentication.
Failed to alloc memory for request sock	Number of memory request failures in the three-way handshake process.
Failed to create open request child	Number of failures to enable subnodes in the three-way handshake process.
SYN ACK retransmits	SYN ACK packet retransmission count.
Timeouted requests	Timeout in the three-way handshake process.
Time-wait	Information about the connection in TIME-WAIT status.
Time-wait bucket table overflow	Overflow statistics of connections in TIME-WAIT status.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 IP REF Commands

Command	Function
clear ip ref packet statistics	Clear the packet statistics of IPv4 REF.
clear ipv6 ref packet statistics	Clear the packet statistics of IPv6 REF.
hash-disturb	Configure the hash disturbance factor of load balancing.
hash-symmetrical	Enable the load balancing hash disturbance function and configure the hash synchronization factor of load balancing, also known as symmetrical hash.
ip ref algorithm mode	Configure the ECMP hash algorithm mode.
ip ref check	Configure illegitimate destination IP address check of IPv4 REF.
ip ref mgmt-forward	Enable L3 forwarding on the management interface.
ip ref load-balance	Configure the ECMP global load balancing algorithm.
ip ref load-sharing	Configure the load balancing algorithm for IPv4 REF.
ip ref hash-elasticity enable	Enable elastic hash of ECMP load balancing.
ip ref synchronize all	Synchronize IPv4 routes between the hardware and software REF.
ip-ref-load-balance-profile	Rename the enhanced profile and enter the enhanced profile configuration mode of REF load balancing.
ipv4 field	Configure the load balancing mode for IPv4 packets in a specified enhanced profile.
ipv6 field	Configure the load balancing mode for IPv6 packets in the specified enhanced profile.
ipv6 ref load-sharing	Set the load balancing algorithm of IPv6 REF to load balancing based on the source and destination IP addresses.
ipv6 ref synchronize all	Synchronize IPv6 routes between the hardware and software REF.
show ip ref adjacency	Display the adjacency table.

show ip ref exact-route	Display the exact forwarding path of an IP packet.
show ip ref load-balance	Display the configuration of the ECMP load balancing.
show ip ref load-balance-profile	Display the configuration of an enhanced profile.
show ip ref packet statistics	Display the packet statistics of IPv4 REF.
show ip ref resolve-list	Display the information actively resolved by IPv4 REF.
show ip ref route	Display all routing information of the current IPv4 REF.
show ip ref route detail	Display the detailed routing table of a specified IPv4 route prefix.
show ipv6 ref adjacency	Display the adjacency information of IPv6 REF.
show ipv6 ref exact-route	Display the actual forwarding path of an IPv6 packet.
show ipv6 ref packet statistics	Display the packet statistics of IPv6 REF.
show ipv6 ref resolve-list	Display the information actively resolved by IPv6 REF.
show ipv6 ref route	Display routing information of IPv6 REF.
show ipv6 ref route detail	Display the detailed routing table of a specified IPv6 route prefix.

1.1 clear ip ref packet statistics

Function

Run the **clear ip ref packet statistics** command to clear the packet statistics of IPv4 REF.

Syntax

clear ip ref packet statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears packet statistics of IPv4 REF.

```
Hostname> enable
Hostname# clear ip ref packet statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear ipv6 ref packet statistics

Function

Run the **clear ipv6 ref packet statistics** command to clear the packet statistics of IPv6 REF.

Syntax

clear ipv6 ref packet statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears packet statistics of IPv6 REF.

```
Hostname> enable
Hostname# clear ipv6 ref packet statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 hash-disturb

Function

Run the **hash-disturb** command to configure the hash disturbance factor of load balancing.

Run the **no** form of this command to disable the load balancing hash disturbance function.

The hash disturbance function of load balancing is disabled by default.

Syntax

hash-disturb *string*

no hash-disturb

Parameter Description

string: Disturbance factor. It is a string of 1 to 16 characters.

Command Modes

Enhanced profile configuration mode of REF load balancing

Default Level

14

Usage Guidelines

Hash disturbance refers that device traffic is balanced using the hash algorithm. For the same stream from two devices of the same type, the same path will be calculated by the load balancing algorithm. When the equal cost multiple path (ECMP) is deployed, the same stream from the two devices may be distributed to the same destination device. This is called hash polarization. The hash disturbance factor is used to affect the load balancing algorithm of the device. Different disturbance factors can be configured on different devices so that different paths are calculated for the same stream.

Examples

The following example configures the hash disturbance factor in enhanced profile configuration mode of REF load balancing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip-ref-load-balance-profile
Warning: The profile default has been created,  and this command will rename it.
Continue? [Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)# hash-disturb A
```

Notifications

When the ECMP hash disturbance factor fails to be configured, the following notification will be displayed:

```
% Set ecmp hash-disturb failed.
```

Platform Description

N/A

Related Commands

- **show ip ref load-balance-profile**

1.4 hash-symmetrical

Function

Run the **hash-symmetrical** command to enable the load balancing hash disturbance function and configure the hash synchronization factor of load balancing, also known as symmetrical hash.

Run the **no** form of this command to disable the load balancing hash disturbance function.

Hash synchronization is enabled by default.

Hash synchronization is disabled by default.

Syntax

hash-symmetrical { **ipv4** | **ipv6** }

no hash-symmetrical { **ipv4** | **ipv6** }

Parameter Description

ipv4: Enables/Disables load balancing hash synchronization for IPv4 packets.

ipv6: Enables/Disables load balancing hash synchronization for IPv6 packets.

Command Modes

Enhanced profile configuration mode of REF load balancing

Default Level

14

Usage Guidelines

To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session be transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. If a traditional hash algorithm is used, the uplink and downlink streams will be directed to different firewalls, while hash synchronization can ensure that the same path is calculated for the uplink and downlink streams.

When hash synchronization is enabled, the source and destination address-based load balancing modes in an enhanced profile need to be configured symmetrically. For example, if load balancing based on source IP addresses is configured, load balancing based on destination IP addresses needs to be configured at the same time.

Examples

The following example enables load balancing hash synchronization for IPv6 packets in enhanced profile configuration mode of REF load balancing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip-ref-load-balance-profile
Warning: The profile default has been created,  and this command will rename it.
Continue? [Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)# hash-symmetrical ipv6
```

Notifications

When load balancing hash synchronization fails to be configured for IPv4 packets, the following notification will be displayed:

```
% Set ecmp hash-symmetrical ipv4 failed.
```

When load balancing hash synchronization fails to be configured for IPv6 packets, the following notification will be displayed:

```
% Set ecmp hash-symmetrical ipv6 failed.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip-ref-load-balance-profile**
- **show ip ref load-balance-profile**

1.5 ip ref algorithm mode

Function

Run the **ip ref algorithm mode** command to configure the ECMP hash algorithm mode.

Run the **no** form of this command to remove this configuration.

Syntax

ip ref algorithm mode *hash-number*

Parameter Description

hash-number: Number of a hash algorithm mode. The value range is from 0 to 9, and the default value is **0**.

When the value is **0**, the hash algorithm mode is x8+x7+x2+x+1.

When the value is **1**, the hash algorithm mode is x8+x7+x6+x+1.

When the value is **2**, the hash algorithm mode is x8.

When the value is **3**, the hash algorithm mode is x10+x3+1.

When the value is **4**, the hash algorithm mode is x10+x7+1.

When the value is **5**, the hash algorithm mode is x16.

When the value is **6**, the hash algorithm mode is x16+x5+x3+x2+1.

When the value is **7**, the hash algorithm mode is x16+x5+x4+x3+1.

When the value is **8**, the hash algorithm mode is x16+x10+x5+x3+1.

When the value is **9**, the hash algorithm mode is x16+x9+x4+x2+1.

hash-number: Number of a hash algorithm mode. The value range is from 3 to 11, and the default value is **9**.

- When the value is **3**, the hash algorithm mode is 16 bit crc16 using bisync polynomial.
- When the value is **4**, the hash algorithm mode is upper 8 bits of crc16 and 8 bit xor1.
- When the value is **5**, the hash algorithm mode is upper 8 bits of crc16 and 8 bit xor2.
- When the value is **6**, the hash algorithm mode is upper 8 bits of crc16 and 8 bit xor4.
- When the value is **7**, the hash algorithm mode is upper 8 bits of crc16 and 8 bit xor8.
- When the value is **8**, the hash algorithm mode is xor16.
- When the value is **9**, the hash algorithm mode is 16 bit crc16 using the ccitt polynomial.
- When the value is **10**, the hash algorithm mode is 16 LSBs of computed crc32.
- When the value is **11**, the hash algorithm mode is 16 MSBs of computed crc32.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to set an appropriate hash algorithm mode to adapt to different traffic models to achieve the optimal load balancing effect.

Examples

The following example sets the number of the ECMP hash algorithm mode to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ref algorithm mode 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ref load-balance**

1.6 ip ref check

Function

Run the **ip ref check** command to configure illegitimate destination IP address check of IPv4 REF.

Run the **no** form of this command to disable this feature.

IPv4 REF does not check illegitimate destination IP addresses by default.

Syntax

ip ref check [**masklen** *mask-length*]

no ip ref check

Parameter Description

masklen *mask-length*: Specifies the IP packet mask length for the illegitimate host address check. The value range is from 1 to 31, and the default value is **24**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

REF can filter out illegitimate class E addresses (excluding 255.255.255.255), addresses with all zeros, and loopback interface addresses (excluding 127.0.0.1), and record the illegitimate destination IP addresses.

Examples

The following example sets the mask length to 20 bits for the illegitimate destination IP address check of IPv4 REF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ref check masklen 20
```

Notifications

N/A

Related Commands

N/A

1.7 ip ref mgmt-forward

Function

Run the **ip ref mgmt-forward** command to enable L3 forwarding on the management interface.

Run the **no** form of this command to disable this feature.

L3 forwarding is enabled on the management interface by default.

Syntax

ip ref mgmt-forward

no ip ref mgmt-forward

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the forwarding function of Ruijie General Operating System (RGOS) is enabled, then L3 forwarding is enabled for both the management interface and other L3 interfaces. If the **no ip ref mgmt-forward** command is run, L3 forwarding can be disabled on the management interface separately without affecting other L3 interfaces. You can run the **ip ref mgmt-forward** command to enable L3 forwarding on the management interface.

If the forwarding function of RGOS is disabled, regardless of whether **no ip ref mgmt-forward** is configured, L3 forwarding is disabled on the management interface and other L3 interfaces.

Examples

The following example disables L3 forwarding on the management interface.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# no ip ref mgmt-forward
```

Notifications

N/A

Related Commands

N/A

1.8 ip ref load-balance

Function

Run the **ip ref load-balance** command to configure the ECMP global load balancing algorithm.

Run the **no** form of this command to restore the default configuration.

The load is balanced according to an enhanced profile by default.

Syntax

ip ref load-balance { **enhanced profile** *profile-name* | **src-dst-ip** | **src-dst-ip-src-dst-l4port** | **src-ip** }

no ip ref load-balance

Parameter Description

enhanced profile *profile-name*: Performs load balancing based on the packet type field configured in the enhanced profile indicated by *profile-name*.

src-dst-ip: Performs load balancing based on the source and destination IP addresses of incoming packets. Packets with different source and destination IP addresses are evenly distributed among member links, while those with the same source and destination IP addresses are distributed to the same member link.

src-dst-ip-src-dst-l4port: Performs load balancing based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of incoming packets.

src-ip: Performs load balancing based on the source IP address of incoming packets. Packets with different source IP addresses are evenly distributed among member links, while those with the same source IP address are distributed to the same member link.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

ECMP differentiates packet flows by using one or several load balancing algorithms based on packet characteristics, such as the source IP address, destination IP address, L4 source port number, and L4

destination port number. It also distributes the same packet flow to the same path for transmission, and different packet flows to equal-cost paths evenly.

For example, in source IP address-based load balancing mode, packets are distributed to different paths based on the source IP addresses of the packets. Packets with different source IP addresses are evenly distributed to equal-cost paths, and packets with the same source IP address are forwarded by the same path.

In an L3 network, you are advised to adopt load balancing based on the source and destination IP addresses of incoming packets.

Examples

The following example configures the ECMP load balancing algorithm based on the source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ref load-balance src-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ref load-balance**

1.9 ip ref load-sharing

Function

Run the **ip ref load-sharing** command to configure the load balancing algorithm for IPv4 REF.

Run the **no** form of this command to restore the default configuration.

The default load balancing algorithm of IPv4 REF is load balancing based on the destination IP addresses of packets.

Syntax

ip ref load-sharing { **original** | **original-only** }

no ip ref load-sharing { **original** | **original-only** }

Parameter Description

original: Sets the load balancing algorithm of IPv4 REF to load balancing based on the source and destination IP addresses.

original-only: Sets the load balancing algorithm of IPv4 REF to load balancing based on the source IP address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

REF is responsible for data forwarding and supports three load balancing algorithms, that is, load balancing based on the destination IP address, load balancing based on the source IP address, and load balancing based on the source and destination IP addresses. When IP packets are forwarded through multiple paths, if the load balancing based on the destination IP address is set, REF will match the destination IP addresses of the packets with one of the paths for forwarding.

Examples

The following example sets the load balancing algorithm of IPv4 REF to load balancing based on the source and destination IP addresses.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ref load-sharing original
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip ref hash-elasticity enable

Function

Run the **ip ref hash-elasticity enable** command to enable elastic hash of ECMP load balancing.

Run the **no** form of this command to restore the default configuration.

Elastic hash of ECMP load balancing is disabled by default.

Syntax

ip ref hash-elasticity enable

no ip ref hash-elasticity enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In normal cases, a load balancing cluster interworks with multiple top of rack (ToR) devices via the ECMP, and the ToR devices are required to distribute all packets of a session to the same scheduling server. However, when a server is faulty, all session streams will be reorganized and balanced according to the traditional load balancing mechanism of ToR devices. In this case, packets of the same session may be distributed to two servers. The elastic hash function ensures that, when one link is faulty, traffic on other links is not affected and only the traffic of the faulty link is distributed to other active links, without affecting the traffic of other links. In this way, traffic of a session will only be distributed to the same server.

Examples

The following example enables the elastic hash of ECMP load balancing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ref hash-elasticity enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ref load-balance**

1.11 ip ref synchronize all

Function

Run the **ip ref synchronize all** command to synchronize IPv4 routes between the hardware and software REF.

Syntax

ip ref synchronize all

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used for routing recovery under faulty conditions. If the hardware fails to install routing entries because the number of existing routing entries exceeds the capacity of the routing table, or routing entries are discarded due to insufficient memory, you can use this command to restore the consistency of routing entries between the hardware and software REF after the number of existing entries is reduced to the normal range.

Examples

The following example synchronizes IPv4 routes between the hardware and software REF.

```
Hostname> enable
Hostname# ip ref synchronize all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip-ref-load-balance-profile

Function

Run the **ip-ref-load-balance-profile** command to rename the enhanced profile and enter the enhanced profile configuration mode of REF load balancing.

Run the **default** form of this command to restore the name of the enhanced profile to **default** and enter the enhanced profile configuration mode of REF load balancing, or restore the default load balancing mode in the enhanced profile.

The default enhanced profile name is **default**.

Syntax

ip-ref-load-balance-profile [*profile-name*]

default ip-ref-load-balance-profile [*profile-name*]

Parameter Description

profile-name: Profile name. It is a string of 1 to 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The device has an enhanced profile named **default**, which cannot be deleted by default.

Run the **ip-ref-load-balance-profile** command (without parameters) to change the profile name to null and enter the enhanced profile configuration mode of REF load balancing.

Run the **ip-ref-load-balance-profile** *profile-name* command (with parameters) to change the profile name to *profile-name* and enter the enhanced profile configuration mode of REF load balancing.

Run the **default ip-ref-load-balance-profile** command (without parameters) to restore the name of the current profile to **default** and enter the enhanced profile configuration mode of REF load balancing.

Run the **default ip-ref-load-balance-profile** *profile-name* command (with parameters) to restore the default load balancing mode for all types of packets in the enhanced profile.

Examples

The following example renames the enhanced profile **rpn**, and enters the enhanced profile configuration mode of REF load balancing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip-ref-load-balance-profile rpn
Warning: The profile default has been used and this command will rename it. Continue?
[Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)#
```

The following example restores the name of the enhanced profile to **default** and restores the default load balancing mode in the enhanced profile.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# default ip-ref-load-balance-profile
Warning: The profile default has been used and this command will rename it. Continue?
[Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)# exit
Hostname(config)# default ip-ref-load-balance-profile default
Hostname(config)# show ip ref load-balance-profile
Load-balance-profile: default
Packet   Hash Field:
   IPV4: src-ip dst-ip l4-src-port l4-dst-port
   IPV6: src-ip dst-ip l4-src-port l4-dst-port
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv4 field**
- **ipv6 field**
- **hash-disturb**
- **hash-symmetrical**
- **show ip ref load-balance-profile**

1.13 ipv4 field

Function

Run the **ipv4 field** command to configure the load balancing mode for IPv4 packets in a specified enhanced profile.

Run the **no** form of this command to restore the default configuration.

The load is balanced based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of packets by default.

Syntax

ipv4 field [**dst-ip**] [**l4-dst-port**] [**l4-src-port**] [**protocol**] [**src-ip**] [**src-port**]

no ipv4 field

Parameter Description

dst-ip: Performs load balancing based on the destination IP addresses of incoming IPv4 packets.

l4-dst-port: Performs load balancing based on the L4 destination port numbers of incoming IPv4 packets.

l4-src-port: Performs load balancing based on the L4 source port numbers of incoming IPv4 packets.

protocol: Performs load balancing based on the protocol types of incoming IPv4 packets.

src-ip: Performs load balancing based on the source IP addresses of incoming IPv4 packets.

src-port: Performs load balancing based on the source port numbers of incoming IPv4 packets.

Command Modes

Enhanced profile configuration mode of REF load balancing

Default Level

14

Usage Guidelines

ECMP differentiates packet flows by using one or several load balancing modes based on packet characteristics, such as the source IP address, destination IP address, L4 source port number, and L4 destination port number. It also distributes the same packet flow to the same path for transmission, and different packet flows to equal-cost paths evenly.

Run the **default ip-ref-load-balance-profile** *profile-name* command (with parameters) to restore the default load balancing mode for all types of packets in the enhanced profile.

Examples

The following example sets the load balancing mode for IPv4 packets to load balancing based on source IP addresses of incoming IPv4 packets in the enhanced profile named rpn.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip-ref-load-balance-profile rpn
Warning: The profile default has been created,  and this command will rename it.
Continue? [Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)# ipv4 field src-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip-ref-load-balance-profile**
- **show ip ref load-balance-profile**

1.14 ipv6 field

Function

Run the **ipv6 field** command to configure the load balancing mode for IPv6 packets in the specified enhanced profile.

Run the **no** form of this command to restore the default configuration.

The load is balanced based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of packets by default.

Syntax

ipv6 field [**dst-ip**] [**l4-dst-port**] [**l4-src-port**] [**protocol**] [**src-ip**] [**src-port**]

no ipv6 field

Parameter Description

dst-ip: Performs load balancing based on the destination IP addresses of incoming IPv6 packets.

l4-dst-port: Performs load balancing based on the L4 destination port numbers of incoming IPv6 packets.

l4-src-port: Performs load balancing based on the L4 source port numbers of incoming IPv6 packets.

protocol: Performs load balancing based on the protocol types of incoming IPv6 packets.

src-ip: Performs load balancing based on the source IP addresses of incoming IPv6 packets.

src-port: Performs load balancing based on the source port numbers of incoming IPv6 packets.

Command Modes

Enhanced profile configuration mode of REF load balancing

Default Level

14

Usage Guidelines

ECMP differentiates packet flows by using one or several load balancing modes based on packet characteristics, such as the source IP address, destination IP address, L4 source port number, and L4 destination port number. It also distributes the same packet flow to the same path for transmission, and different packet flows to equal-cost paths evenly.

Run the **default ip-ref-load-balance-profile** *profile-name* command (with parameters) to restore the default load balancing mode for all types of packets in the enhanced profile.

Examples

The following example sets the load balancing mode for IPv6 packets to load balancing based on source IP addresses of incoming IPv6 packets in the enhanced profile named rpn.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip-ref-load-balance-profile rpn
Warning: The profile default has been created,  and this command will rename it.
Continue? [Y/N]:Y
Hostname(ref-ip-config-load-balance-profile)# ipv6 field src-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip-ref-load-balance-profile**
- **show ip ref load-balance-profile**

1.15 ipv6 ref load-sharing

Function

Run the **ipv6 ref load-sharing** command to set the load balancing algorithm of IPv6 REF to load balancing based on the source and destination IP addresses.

Run the **no** form of this command to restore the default configuration.

The default load balancing algorithm of IPv6 REF is load balancing based on the destination IPv6 address.

Syntax

ipv6 ref load-sharing { **original** | **original-only** }

no ipv6 ref load-sharing { **original** | **original-only** }

Parameter Description

original: Sets the load balancing algorithm of IPv6 REF to load balancing based on the source and destination IP addresses.

original-only: Sets the load balancing algorithm of IPv6 REF to load balancing based on the source IP address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

REF is responsible for data forwarding and supports three load balancing algorithms, that is, load balancing based on the destination IP address, load balancing based on the source IP address, and load balancing based on the source and destination IP addresses. When IP packets are forwarded through multiple paths, if the load balancing based on the destination IP address is set, REF will match the destination IP addresses of the packets with one of the paths for forwarding.

Examples

The following example sets the load balancing algorithm of IPv6 REF to load balancing based on the source and destination IP addresses.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 ref load-sharing original
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ipv6 ref synchronize all

Function

Run the **ipv6 ref synchronize all** command to synchronize IPv6 routes between the hardware and software REF.

Syntax

ipv6 ref synchronize all

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used for routing recovery under faulty conditions. If the hardware fails to install routing entries because the number of existing routing entries exceeds the capacity of the routing table, or routing entries are discarded due to insufficient memory, you can use this command to restore the consistency of routing entries between the hardware and software REF after the number of existing entries is reduced to the normal range.

Examples

The following example synchronizes the IPv6 routes between the hardware and software REF.

```
Hostname> enable
Hostname# ipv6 ref synchronize all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 show ip ref adjacency

Function

Run the **show ip ref adjacency** command to display the adjacency table.

Syntax

show ip ref adjacency [**glean** | **local** | *ip-address* | **interface** *interface-type interface-number* | **discard** | **statistics**]

Parameter Description

glean: Indicates glean adjacent nodes.

local: Indicates local adjacent nodes.

ip-address: Adjacency next-hop IP address.

interface *interface-type interface-number*: Specifies the interface type and interface number.

discard: Displays the adjacent nodes that are discarded.

statistics: Displays statistics.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command displays the current adjacency table of IPv4 REF. You can specify parameters to check the glean adjacencies, local adjacencies, adjacency of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes.

Examples

The following example displays information about all the current adjacent nodes.

```
Hostname> enable
Hostname# show ip ref adjacency
id state     type    rfct chg  ip          interface       linklayer(header data)
1  unresolved mcast   1    0   224.0.0.0
9  resolved   forward 1    0   192.168.50.78   GigabitEthernet 0/0  00 25 64 C5 9D 6A
00 D0 F8 98 76 54 08 00
7  resolved   forward 1    0   192.168.50.200  GigabitEthernet 0/0  00 04 5F 87 69 66
00 D0 F8 98 76 54 08 00
6  unresolved  glean  1    0   0.0.0.0        GigabitEthernet 0/0
4  unresolved  local  3    0   0.0.0.0        Local 1
```

Table 1-1 Output Fields of the show ip ref adjacency Command

Field	Description
id	Adjacency ID.
state	Adjacency status. ● **unresolved**: Indicates unresolved. ● **resolved**: Indicates resolved.

Field	Description
type	Adjacency type. ● **local**: Indicates a local adjacency. ● **forward**: Indicates a forwarding adjacency. ● **discard**: Indicates a discarded adjacency. ● **glean**: Indicates a glean adjacency. ● **mcast**: Indicates a multicast adjacency.
rfct	Number of times that an adjacency is referenced.
chg	Whether an adjacency is in the change chain.
ip	IP address of an adjacency.
interface	Outbound interface.
linklayer(header data)	L2 header.

Notifications

N/A

Platform Description

N/A

1.18 show ip ref exact-route

Function

Run the **show ip ref exact-route** command to display the exact forwarding path of an IP packet.

Syntax

show ip ref exact-route [**vrf** *vrf-name*] *source-ip-address destination-ip-address*

Parameter Description

vrf *vrf-name*: Indicates the name of a VRF instance.

source-ip-address: Source IP address of a packet.

destination-ip-address: Destination IP address of a packet.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command displays the forwarding path of a packet whose source and destination IP addresses are specified.

Examples

The following example displays the exact forwarding path of a packet with the source IP address 192.168.217.74 and destination IP address 192.168.13.1.

```
Hostname> enable
Hostname# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74  --> 192.168.13.1 (vrf global):
id state    type    rfct chg  ip          interface        linklayer(header data)
9  resolved forward 1     0   192.168.17.1  GigabitEthernet 0/0 00 25 64 C5 9D 6A 00
D0 F8 98 76 54 08 00
```

Table 1-2 Output Fields of the show ip ref exact-route Command

Field	Description
id	Adjacency ID.
state	Adjacency status. ● **unresolved**: Indicates unresolved. ● **resolved**: Indicates resolved.
type	Adjacency type. ● **local**: Indicates a local adjacency. ● **forward**: Indicates a forwarding adjacency. ● **discard**: Indicates a discarded adjacency. ● **glean**: Indicates a glean adjacency. ● **mcast**: Indicates a multicast adjacency.
rfct	Number of times that an adjacency is referenced.
chg	Whether an adjacency is in the change chain.
ip	IP address of an adjacency.
interface	Outbound interface.
linklayer(header data)	L2 header.

Notifications

N/A

Platform Description

N/A

1.19 show ip ref load-balance

Function

Run the **show ip ref load-balance** command to display the configuration of the ECMP load balancing.

Syntax

show ip ref load-balance

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of the ECMP load balancing.

```
Hostname> enable
Hostname# show ip ref load-balance
  load-balance          : enhanced profile.
  hash-elasticity       : disable.
```

Table 1-3 Output Fields of the show ip ref load-balance Command

Field	Description
load-balance	Type of the configured ECMP load balancing algorithm.
hash-elasticity	• **enable**: Indicates that elastic hash is supported. • **disable**: Indicates that elastic hash is not supported.

Notifications

N/A

Platform Description

N/A

1.20 show ip ref load-balance-profile

Function

Run the **show ip ref load-balance-profile** command to display the configuration of an enhanced profile.

Syntax

show ip ref load-balance-profile [*profile-name*]

Parameter Description

profile-name: Profile name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If *profile-name* is not specified, information about all enhanced profiles will be displayed.

Examples

The following example displays the enhanced load balancing configuration of the enhanced profile named rpn.

```
Hostname> enable
Hostname# show ip ref load-balance-profile rpn
Load-balance-profile: rpn
Packet   Hash Field:
   IPV4: src-ip dst-ip l4-src-port l4-dst-port
   IPV6: src-ip dst-ip l4-src-port l4-dst-port
```

Table 1-4 Output Fields of the show ip ref load-balance-profile Command

Field	Description
Load-balance-profile	Name of an enhanced profile.
Packet	Packet type. ● **IPv4**: Indicates the load balancing configuration for IPv4 packets in an enhanced profile. ● **IPv6**: Indicates the load balancing configuration for IPv6 packets in an enhanced profile.
Hash Field	Load balancing mode.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip-ref-load-balance-profile**
- **ipv4 field**
- **ipv6 field**
- **hash-disturb**
- **hash-symmetrical**

1.21 show ip ref packet statistics

Function

Run the **show ip ref packet statistics** command to display the packet statistics of IPv4 REF.

Syntax

show ip ref packet statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays packet statistics of IPv4 REF.

```
Hostname> enable
Hostname# show ip ref packet statistic
IPv4 REF Packet Statistics:
   Flags forward    : 0
   Ip head option   : 68
   Lookup FIB fail  : 0
   Deny forward     : 0
   Invalid adj id   : 0
   Glean adj        : 0
   TTL expiration   : 0
   Don't fragment   : 0
   Ip redirect      : 0
```

```
Redirect p2p    : 0
Forward adj     : 0
Vxlan adj       : 0
Local adj       : 43026
Mcast reserved  : 180
Punt adj        : 0
Cached reserve  : 0
Cached drop     : 0
Cached lost     : 0
Null interface  : 0
Total packets   : 45547
redirect drop   : 0
```

Table 1-5 Output Fields of the show ip ref packet statistics Command

Field	Description
IPv4 REF Packet Statistics	Packet statistics of IPv4 REF.
Flags forward	Number of routed packets.
Ip head option	Number of IP packets with options.
Lookup FIB fail	Number of packets with failed REF routing.
Deny forward	Number of packets that are discarded due to no IP routing.
Invalid adj id	Invalid adjacency index.
Glean adj	Number of packets that match glean adjacencies.
TTL expiration	Number of packets with TTL timeout.
Don't fragment	Number of packets that are discarded because they cannot be fragmented.
Ip redirect	Number of packets that are redirected.
Redirect p2p	Number of packets that are redirected in a point-to-point way.
Forward adj	Number of packets that match forwarding adjacencies.
Vxlan adj	Number of packets that match VXLAN adjacencies.
Local adj	Number of packets that match local adjacencies.
Mcast reserved	Number of packets that are sent by the multicast service to the process.
Punt adj	Number of packets that match Punt adjacencies.
Cached reserve	Number of packets that are sent to the process after cached.
Cached drop	Number of packets that are discarded after cached.
Cached lost	Number of packets that are cached.
Null interface	Number of packets that hit the NULL 0 egress.

Field	Description
Total packets	Total number of packets that are sent to the REF module.
redirect drop	Number of packets that are discarded due to reverse path limited (RPL).

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show ip ref resolve-list

Function

Run the **show ip ref resolve-list** command to display the information actively resolved by IPv4 REF.

Syntax

show ip ref resolve-list

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information actively resolved by IPv4 REF.

```
Hostname> enable
Hostname# show ip ref resolve-list
IP            State    Flags  Interface
1.1.1.1        unres    1     GigabitEthernet 0/0
```

Table 1-6 Output Fields of the show ip ref resolve-list Command

Field	Description

Field	Description
IP	IP address.
State	• **unres**: Indicates unresolved. • **res**: Indicates resolved.
Flags	• **0**: Indicates unrelated to adjacencies. • **1**: Indicates related to adjacencies.
Interface	Interface name

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 show ip ref route

Function

Run the **show ip ref route** command to display all routing information of the current IPv4 REF.

Syntax

show ip ref route [**vrf** *vrf-name*] [**default** | *ipv4-address mask* | **statistics**]

Parameter Description

vrf *vrf-name*: Displays routing information of a specified VRF instance.

default: Specifies the default route.

ipv4-address: Destination IP address of a specified route.

mask: Mask of a specified route.

statistics: Displays statistics.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the routing information of the current IPv4 REF. You can specify parameters so that information about the default route, the route of a specified IP/mask, or all routes is displayed.

Examples

The following example displays all routing information of the current IPv4 REF.

```
Hostname> enable
Hostname# show ip ref route
Codes: * - default route
      # - zero route
 ip/mask          weight  path-id     next-hop       interface
 255.255.255.255/32 1      4          0.0.0.0        Local 1
 224.0.0.0/24      1      4          0.0.0.0        Local 1
 192.168.50.0/24    1      6          0.0.0.0        GigabitEthernet 0/0
 192.168.50.200/32  1      7          192.168.50.200  GigabitEthernet 0/0
 192.168.50.122/32  1      4          0.0.0.0        Local 1
 192.168.50.78/32   1      9          192.168.50.78   GigabitEthernet 0/0
```

Table 1-7 Output Fields of the show ip ref route Command

Field	Description
ip/mask	Destination IP address and mask length.
path-id	Adjacency index ID.
weight	Weight value of a route.
next_hop	Next hop
interface	Outbound interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.24 show ip ref route detail

Function

Run the **show ip ref route detail** command to display the detailed routing table of a specified IPv4 route prefix.

Syntax

show ip ref route detail *ip-address* [**vrf** *vrf-name*]

Parameter Description

ip-address: IP address.

vrf *vrf-name*: Indicates the name of a VRF instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the detailed routing table of a specified route prefix.

Examples

The following example displays the detailed routing table of the IPv4 route prefix 100.0.0.0.

```
Hostname> enable
Hostname# show ip ref route detail 100.0.0.0
IPv4 100.000.000.000/8 vrf:0
================================ SSC INFO ================================
    ifx nh_ip          pri w mac           cmd    vid  l2_ifx sub_port main_vid rt_type
rt_own
[ 0] 28  054.000.000.002 0   1 0000.0011.1111 forward  0  0     0       0
local_adj comm
[ 1] 29  055.000.000.002 0   1 0000.0000.0055 forward  0  0     0       0
local_adj comm
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSC END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
================================ SSD INFO ================================
***** LC slot 1/5 ROUTE INFO *****
 prefix_type nh_id  ecmp_gid owner  ecmp_ready    nhblk_id nh_id nhblk_ready
 lpm        9     1       comm   1            9       9    1
    ifx ip           intf_id phyid    vlan  cmd   flow_id  mac           adj_id
in_adj_id nhitem_id nh_status
[ 0] 28  054.000.000.002 1      0x7001f04 4094 forward 0      0000.0011.1111  0     0
0        1
[ 1] 29  055.000.000.002 2      0x7001f05 4093 forward 0      0000.0000.0055  0     0
0        1
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSD END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
================================ SSA INFO ================================
***** LC slot 1/5 ROUTE INFO *****
[unit:0] hw_type:lpm ecmpgid:1 nh_id:9 flowid:4 hit:[2048]0
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSA END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Table 1-8 Output Fields of the show ip ref route detail Command

Field	Description
ifx	Interface ID.
nh_ip	IP address of the next hop.

Field	Description
pri	Priority of the next hop.
w	Weight value of the next hop.
mac	MAC address of the next hop.
cmd	Adjacency forwarding action.
vid	VLAN ID.
l2_ifx	Physical port number.
sub_port	VXLAN subinterface.
main_vid	Primary VLAN ID.
rt_type	Route type.
rt_own	Network, to which a route belongs.
prefix_type	Prefix type.
nh_id	Resource IP address of the next hop.
ecmp_gid	Resource ID of an ECMP group.
ecmp_ready	Resource readiness identifier of an ECMP group.
nhblk_id	Next-hop block ID.
nhblk_ready	Next-hop resource readiness identifier.
intf_id	RIF resource ID.
phyid	Physical port ID.
vlan	Actual VLAN.
flow_id	Flow classification ID.
adj_id	Adjacency resource ID.
in_adj_id	ID of the resource, to which the inner adjacency belongs.
nhitem_id	ID of the resource, to which the next-hop member belongs.
nh_status	Action flag of the next hop. ● **forward**: Indicates packet forwarding. ● **drop**: Indicates discarding.
unit	ID of the installed chip.
hit	Flow hit identifier.

Notifications

When a route does not exist, or the search times out or fails, the following notification will be displayed:

```
% ROUTE INFO NOT FOUND, FOR NO ROUTE HITTED OR LOOK UP TIME OUT
```

Platform Description

N/A

Related Commands

N/A

1.25 show ipv6 ref adjacency

Function

Run the **show ipv6 ref adjacency** command to display the adjacency information of IPv6 REF.

Syntax

show ipv6 ref adjacency [**glean** | **local** | *ipv6-address* | **interface** *interface-type interface-number* | **discard** | **statistics**]

Parameter Description

glean: Displays glean adjacent nodes.

local: Displays local adjacent nodes.

ipv6-address: IPv6 address. After this parameter is configured, adjacency information of a specified address (x:x:x:x::x) will be displayed.

interface *interface-type interface-number*: Specifies the interface type and interface number.

discard: Displays the adjacent nodes that are discarded.

statistics: Displays the statistics on all types of adjacencies.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command displays the current adjacency table of IPv6 REF. You can specify parameters to check glean adjacencies, local adjacencies, adjacency of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes.

Examples

The following example displays adjacencies of IPv6 REF.

```
Hostname> enable
Hostname# show ipv6 ref adjacency
id    state      type    rfct chg ip    interface          linklayer(header data)
```

```
1    unresolved  glean   1    0   ::    GigabitEthernet 0/0
2    unresolved  local   2    0   ::1   Local 1
```

Table 1-9 Output Fields of the show ipv6 ref adjacency Command

Field	Description
id	ID of an adjacent node.
state	State of an adjacent node.
type	Type of an adjacent node. ● **local**: Indicates a local adjacency. ● **forward**: Indicates a forwarding adjacency. ● **discard**: Indicates a discarded adjacency. ● **glean**: Indicates a glean adjacency. ● **mcast**: Indicates a multicast adjacency.
rfct	Number of times that the route of an adjacent node is referenced.
chg	● **0**: Indicates that an adjacent node is not in the adjacency change chain. ● **1**: Indicates that an adjacent node is in the adjacency change chain.
ip	IPv6 address of an adjacency.
interface	Physical port associated with an adjacent node.
linklayer(header data)	L2 header filling information.

Note

For a distributed device, the **id** column contains two fields: **gid** and **lid**, of which **gid** indicates the global adjacent node ID and **lid** indicates the local adjacent node ID.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show ipv6 ref exact-route

Function

Run the **show ipv6 ref exact-route** command to display the actual forwarding path of an IPv6 packet.

Syntax

show ipv6 ref exact-route [**vrf** *vrf-name*] *source-ipv6-address destination-ipv6-address*

Parameter Description

vrf *vrf-name*: Indicates the name of a VRF instance.

source-ipv6-address: Source IPv6 address.

destination-ipv6-address: Destination IPv6 address.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the actual forwarding path of a packet with the source address 2001:db8:1::1 and the destination address 3001:db8:2::2.

```
Hostname> enable
Hostname# show ipv6 ref exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2 (vrf global):
ID  state      type    rfct chg ip interface           linklayer(header data)
3   unresolve   glean   1    0   :: GigabitEthernet 0/0
```

Table 1-10 Output Fields of the show ipv6 ref exact-route Command

Field	Description
id	ID of an adjacent node.
state	State of an adjacent node.
type	Type of an adjacent node. ● **local**: Indicates a local adjacency. ● **forward**: Indicates a forwarding adjacency. ● **discard**: Indicates a discarded adjacency. ● **glean**: Indicates a glean adjacency. ● **mcast**: Indicates a multicast adjacency.

Field	Description
rfct	Number of times that the route of an adjacent node is referenced.
chg	• **0**: Indicates that an adjacent node is not in the adjacency change chain. • **1**: Indicates that an adjacent node is in the adjacency change chain.
ip	IPv6 address of an adjacency.
interface	Physical port associated with an adjacent node.
linklayer(header data)	L2 header filling information.

Note

For a distributed device, the **id** column contains two fields: **gid** and **lid**, of which **gid** indicates the global adjacent node ID and **lid** indicates the local adjacent node ID.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show ipv6 ref packet statistics

Function

Run the **show ipv6 ref packet statistics** command to display the packet statistics of IPv6 REF.

Syntax

show ipv6 ref packet statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays packet statistics of IPv6 REF.

```
Hostname> enable
Hostname# show ipv6 ref packet statistics
IPv6 REF Packet Statistics:
   Flags forward   : 0
   Payload big     : 0
   Dstaddr multi   : 18558
   Param err       : 0
   Lookup fib fail  : 0
   Null Dstintf    : 0
   No ipv6 pkt     : 0
   Deny forward    : 0
   TTL expirate    : 0
   Packet too big   : 0
   Address bscope   : 0
   Redirect packet  : 0
   Glean adj       : 0
   Forward adj     : 0
   Local adj       : 649
   Vxlan adj       : 0
   Punt adj        : 0
   Mcast adj       : 0
   Discard adj     : 0
   Cached drop     : 0
   Cached lost     : 0
   Cached rsvd     : 0
   Current cache pkt: 0
   Total packets   : 19207
```

Table 1-11 Output Fields of the show ipv6 ref packet statistics Command

Field	Description
IPv6 REF Packet Statistics	Statistics on packets of IPv6 REF.
Flags forward	Number of routed packets.
Payload big	Number of packets with the actual length smaller than the maximum packet length under load balancing.
Dstaddr multi	Number of packets with the destination addresses being multicast addresses.
Param err	Number of packets with illegitimate parameters (for example, VRF).
Lookup fib fail	Number of packets with failed REF routing.
Null Dstintf	Number of packets with the destination egress being null.

Field	Description
No ipv6 pkt	Number of non-IPv6 packets.
Deny forward	Number of packets that are denied for forwarding.
TTL expirate	Number of packets with abnormal TTL.
Packet too big	Number of packets that are discarded due to too large size.
Address bscope	Number of packets beyond the scope of source address.
Redirect packet	Number of packets that are redirected.
Glean adj	Number of packets that match glean adjacencies.
Forward adj	Number of packets that match forwarding adjacencies.
Local adj	Number of packets that match local adjacencies.
Vxlan adj	Number of packets that match VXLAN adjacencies.
Punt adj	Number of packets that match Punt adjacencies.
Mcast adj	Number of packets that match multicast adjacencies.
Discard adj	Number of packets that match discarded adjacencies.
Cached drop	Number of packets that are discarded after cached.
Cached lost	Number of packets that are cached.
Cached rsvd	Number of packets that are sent to the process after cached.
Current cache pkt	Number of packets that are being cached.
Total packets	Total number of packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show ipv6 ref resolve-list

Function

Run the **show ipv6 ref resolve-list** command to display the information actively resolved by IPv6 REF.

Syntax

show ipv6 ref resolve-list

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information actively resolved by IPv6 REF.

```
Hostname> enable
Hostname# show ipv6 ref resolve-list
IP              State    Flags   Interface
1000::1          unres    1     GigabitEthernet 0/0
```

Table 1-12 Output Fields of the show ipv6 ref resolve-list Command

Field	Description
IP	IPv6 address of an interface.
State	● **unres**: Indicates unresolved. ● **res**: Indicates resolved.
Flags	● **0**: Indicates unrelated to adjacencies. ● **1**: Indicates related to adjacencies.
Interface	Interface name

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show ipv6 ref route

Function

Run the **show ipv6 ref route** command to display routing information of IPv6 REF.

Syntax

show ipv6 ref route [**vrf** *vrf-name*] [**default** | **statistics** | *ipv6-address/prefix-length*]

Parameter Description

vrf *vrf-name*: Indicates the name of a VRF instance.

default: Displays the information of the default route.

statistics: Displays the route statistics.

ipv6-address/prefix-length: Prefix. After this parameter is configured, the routing information of a specified prefix (X:X:X:X::X/<0-128>) is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display routing information of IPv6 REF. When no VRF parameter is specified, the global routing table is queried; when the VRF parameter is specified, the related VRF routing table is queried.

You can specify parameters to check information about the default route, the route with a specified prefix, or the statistics on all routes.

Examples

The following example displays routing information of IPv6 REF.

```
Hostname> enable
Hostname# show ipv6 ref route
Codes: * - default route
 prefix/len                  weight path_id  next_hop interface
 2001:da8:ffe:2::/64           1       3      ::     GigabitEthernet 0/0
 2001:da8:ffe:2::3/128         1       2      ::1    Local 1
 fe80::/10                   1       6      ::     Null 0
 fe80::21a:a9ff:fe3b:fa41/128   1       2       ::1    Local 1
```

Table 1-13 Output Fields of the show ipv6 ref route Command

Field	Description
prefix/len	IPv6 prefix and prefix length.
weight	Weight value of a route.
path_id	Adjacency index ID.

Field	Description
next_hop	Next-hop address
interface	Name of the interface associated with an adjacent node.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 show ipv6 ref route detail

Function

Run the **show ipv6 ref route detail** command to display the detailed routing table of a specified IPv6 route prefix.

Syntax

show ipv6 ref route detail *ipv6-address* [**vrf** *vrf-name*]

Parameter Description

ipv6-address: IPv6 address.

vrf *vrf-name*: Indicates the name of a VRF instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the detailed routing table of a specified route prefix.

Examples

The following example displays the detailed routing table of the IPv6 route prefix 120::.

```
Hostname> enable
Hostname# show ipv6 ref route detail 120::
IPv6 120::/32 vrf:0
================================ SSC INFO ================================
    ifx nh_ip  pri w   mac            cmd       vid   l2_ifx sub_port main_vid rt_type
rt_own
```

```
[ 0] 244 38::2  0   1   0000.6638.3838   forward    0     0      0       0
local_adj comm
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSC END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
============================== SSD INFO ==============================
***** LC slot 1/3 ROUTE INFO *****
 prefix_type nh_id  ecmp_gid owner  ecmp_ready    nhblk_id nh_id nhblk_ready
 lpm        11     0       comm   1            0       11    1
    ifx ip    intf_id phyid    vlan cmd   flow_id mac          adj_id in_adj_id
nhitem_id nh_status
[ 0] 244 38::2 5      0x7001d30 4094 forward  0     0000.6638.3838  0     0        0
1
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSD END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
============================== SSA INFO ==============================
***** LC slot 1/3 ROUTE INFO *****
[unit:0] hw_type:lpm ecmpgid:0 nh_id:11 flowid:4 hit:[17]0
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSA END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ SSA END ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Table 1-14 Output Fields of the show ipv6 ref route detail Command

Field	Description
ifx	Interface ID.
nh_ip	IP address of the next hop.
pri	Priority of the next hop.
w	Weight value of the next hop.
mac	MAC address of the next hop.
cmd	Adjacency forwarding action.
vid	VLAN ID.
l2_ifx	Physical port number.
sub_port	VXLAN subinterface.
main_vid	Primary VLAN ID.
rt_type	Route type.
rt_own	Network, to which a route belongs.
prefix_type	Prefix type.
nh_id	Resource IP address of the next hop.
ecmp_gid	Resource ID of an ECMP group.
ecmp_ready	Resource readiness identifier of an ECMP group.

Field	Description
nhblk_id	Next-hop block ID.
nhblk_ready	Next-hop resource readiness identifier.
intf_id	RIF resource ID.
phyid	Physical port ID.
vlan	Actual VLAN.
flow_id	Flow classification ID.
adj_id	Adjacency resource ID.
in_adj_id	ID of the resource, to which the inner adjacency belongs.
nhitem_id	ID of the resource, to which the next-hop member belongs.
nh_status	Action flag of the next hop. ● **forward**: Indicates packet forwarding. ● **drop**: Indicates discarding.
unit	ID of the installed chip.
hit	Flow hit identifier.

Notifications

When a route does not exist, or the search times out or fails, the following notification will be displayed:

```
% ROUTE INFO NOT FOUND, FOR NO ROUTE HITTED OR LOOK UP TIME OUT
```

Platform Description

N/A

Related Commands

N/A

IP Routing Commands

1 IP Routing Basic Commands

Command	Function
clear ip route	Clear the routing table cache. You can run this command in privileged EXEC mode.
ip recur-route fastswitch-nexthop	Enable fast convergence of recursive routing.
ip recur-route over default-route disable	Configure the function of forbidding recursion to the default route.
ip route arp-to-host delay-time	Configure the delayed redistribution of ARP-to-host route.
ip route arp-to-host interface	Enable ARP-to-host conversion on the specified interface.
ip route arp-to-host tag	Configure the tag attribute of the host route converted by ARP.
ip route notify delete always	Configure direct deletion of the Border Gateway Protocol (BGP) route during graceful restart (GR).
ip routing	Enable the IP routing function of a device.
ipv6 recur-route fastswitch-nexthop	Enable fast convergence of recursive routing.
ipv6 route nd-to-route delay-time	Configure delayed redistribution of the routes converted by neighbor discovery (ND).
ipv6 route nd-to-route interface	Enable ND conversion to a route with fixed-length mask on the specified interface.
ipv6 route nd-to-route tag	Configure the tag attribute of the ND-converted route.
ipv6 route nd-to-route warning-ignore	Configure the function of ignoring warning log of ND conversion to a route of specified length.
ipv6 unicast-routing	Enable the IPv6 routing function of a device.
maximum-paths	Configure the number of equal-cost routes.
show ip route	Display IP routing table information, as well as the equal-cost multi-path routing (ECMP) attribute of routes.
show ip route recursive	Display the recursive information of an IP route.

show ip route static bfd	Display the BFD correlation information of an IP route.
show ip route summary	Display the statistics of a single routing table.
show ip route track-table	Display the track correlation information of an IP route.
show ipv6 route	Display the routing information of an IPv6 route.
show ipv6 route static bfd	Display the BFD correlation information of an IPv6 route.
show ipv6 route summary	Display the statistics of a single IPv6 routing table.
show route-res usage	Display the usage of routing resources.

1.1 clear ip route

Function

Run the **clear ip route** command to clear the routing table cache. You can run this command in privileged EXEC mode.

Syntax

clear ip route [**vrf** *vrf-name*] { ***** | *network* [*mask*] }

Parameter Description

vrf *vrf-name*: Clears the route cache of the specified VRF instance. If virtual routing and forwarding (VRF) is not specified, the command is executed on all VRFs.

*: Clears all the route caches.

network: Network or subnet address for cache clearing.

mask: Network mask. When no mask is specified, the *network* value is used to match the longest route entry in the routing table and clear the cache.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Clearing route cache will delete the corresponding route, and then trigger relearning of the routing protocol. Note that, if the cache of the whole routing table is cleared, the communication of the entire network will be interrupted temporarily.

Examples

The following example clears the cache of the longest routing table entry matched with 192.168.12.0.

```
Hostname> enable
Hostname# clear ip route 192.168.12.0
```

Notifications

N/A

Platform Description

N/A

1.2 ip recur-route fastswitch-nexthop

Function

Run the **ip recur-route fastswitch-nexthop** command to enable fast convergence of recursive routing.

Run the **no** form of this command to disable fast convergence of recursive routing.

Run the **default** form of this command to restore the default configuration.

The fast convergence function of recursive routing is disabled by default.

Syntax

ip recur-route fastswitch-nexthop

no ip recur-route fastswitch-nexthop

default ip recur-route fastswitch-nexthop

Parameter Description

N/A

Command Modes

Global configuration mode

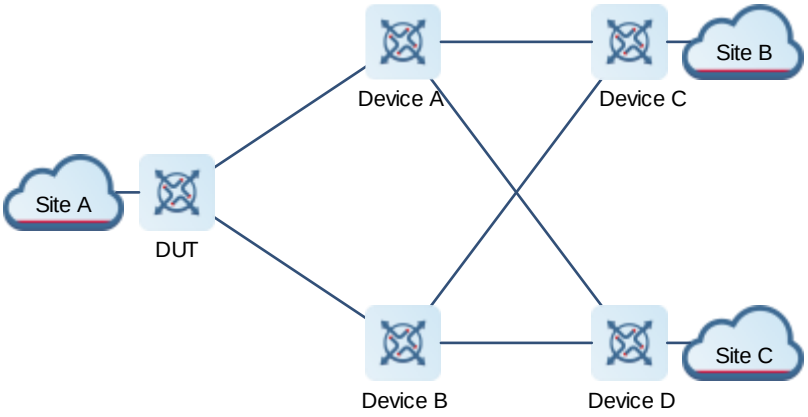
Default Level

14

Usage Guidelines

When link discovery changes or is interrupted, the recursive routing query of dynamic route may converge 2 seconds later. The convergence time is intolerable in some scenarios with high reliability requirements. When the fast convergence function of recursive routing is enabled, the intermediate next hop information will be added to the route sending information. Even if the intermediate link fails, it can be sensed by routing management to shorten the convergence time.

Figure 1-1 Fast Convergence Diagram of IPv4 Recursive Routing



As shown in Figure 1-1, the device under test (DUT) establishes an Intermediate System to Intermediate System (IS-IS) neighbor relationship with Device A and Device B respectively, Device A and Device B establish an IS-IS neighbor relationship with Device C and Device D respectively, and DUT establishes an Internal Border Gateway Protocol (IBGP) neighbor relationship with Device C and Device D respectively. Service sites access the network via External Border Gateway Protocol (EBGP).

In the scenario shown above, BGP routes may be recursed to IS-IS routes. When the link between Device A and Device C is disconnected, the IS-IS route will change and the BGP route that relies on the IS-IS route needs to be re-calculated. Before the calculation result is delivered to the forwarding plane, the BGP traffic from

Site A to Site B still goes through the disconnected link between Device A and Device C, resulting in traffic interruption. Traffic interruption duration = Link down time + Time required by the local IS-IS system to learn route deletion information + Time required by the local NSM system to receive IS-IS routing information + Time required for calculating the BGP route and delivering the result to the forwarding plane + Link switching time. The switching cannot be completed within 1 second.

If the fast convergence function of recursive routing is enabled, the traffic that needs to go through the disconnected link between Device A and Device C can be switched to a normal link within 1 second.

Examples

The following example enables the fast convergence function of recursive routing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip recur-route fastswitch-nexthop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip recur-route over default-route disable

Function

Run the **ip recur-route over default-route disable** command to configure the function of forbidding recursion to the default route.

Run the **no** form of this command to disable the function of forbidding recursion to the default route.

Run the **default** form of this command to restore the default configuration.

Recursion to the default route is allowed by default.

Syntax

ip recur-route over default-route disable

no ip recur-route over default-route disable

default ip recur-route over default-route disable

Parameter Description

N/A

Command Modes

Global configuration mode

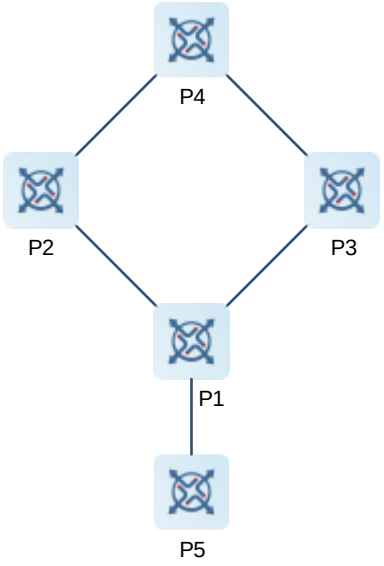
Default Level

14

Usage Guidelines

When you do not want to use the default route for service traffic, you can configure this command to not select the default route egress in recursive routing.

Figure 1-2 Diagram for Forbidding Recursion to Default Route



As shown in Figure 1-2, P1 establishes a non-direct EBGP neighbor relationship with P2 and P3 respectively, service traffic on P1 is balanced and distributed to P4 through P2 and P3. The default route configured on P1 is used to access the Internet through the P1-P5 link egress. When the link between P1 and P2 is faulty, it is expected that service traffic be switched to P3. However, some service traffic is guided to the P1-P5 egress due to the existence of the default route. The P1-P5 egress is not a service egress. As a result, some service traffic is lost and the convergence cannot be completed within 1 second.

With this command, when the link between P1 and P2 is faulty, traffic is completely switched to P3 and is not guided to P5, achieving convergence within 1 second.

Note: When the egress of a default route is not the expected service egress, this command must be configured.

Examples

The following example forbids recursion to the default route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip recur-route over default-route disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip route arp-to-host delay-time

Function

Run the **ip route arp-to-host delay-time** command to configure the delayed redistribution of ARP-to-host route.

Run the **no** form of this command to delete the delayed redistribution of ARP-to-host route.

Run the **default** form of this command to restore the default configuration.

The delayed redistribution function of ARP-to-host route is disabled by default.

Syntax

ip route arp-to-host delay-time *time-number*

no ip route arp-to-host delay-time

default ip route arp-to-host delay-time

Parameter Description

time-number: Delayed redistribution time of ARP-to-host route, in seconds. The value range is from 1 to 1000, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent route jitter caused by change to an Address Resolution Protocol (ARP) entry, you can delay conversion of the ARP entry into a route.

Note

After delayed redistribution is configured, redistribution of a route with effective ARP will be delayed according to the specified delay time. For a route with invalid ARP, advertising of the redistribution withdrawal route is not controlled, and the route will be advertised immediately.

Examples

The following example configures delayed redistribution of the ARP-to-host route.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ip route arp-to-host delay-time 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip route arp-to-host interface

Function

Run the **ip route arp-to-host interface** command to enable ARP-to-host conversion on the specified interface.

Run the **no** form of this command to disable ARP-to-host conversion on the specified interface.

Run the **default** form of this command to restore the default configuration.

The ARP-to-host conversion function is disabled on an interface by default.

Syntax

ip route arp-to-host interface *interface-type interface-number*

no ip route arp-to-host interface *interface-type interface-number*

default ip route arp-to-host interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Note

When configuring this command, make sure that the interface is a Layer-3 interface.

Examples

The following example enables ARP-to-host conversion on the interface of VLAN 40.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip route arp-to-host interface vlan 40
```

Notifications

N/A

Common Errors

If the Layer-3 interface is not up, this function is unavailable.

Platform Description

N/A

Related Commands

N/A

1.6 ip route arp-to-host tag

Function

Run the **ip route arp-to-host tag** command to configure the tag attribute of the host route converted by ARP.

Run the **no** form of this command to delete the tag attribute of the host route converted by ARP.

Run the **default** form of this command to restore the default configuration.

The tag attribute function of the host route is disabled by default.

Syntax

ip route arp-to-host tag *tag-number*

no ip route arp-to-host tag *tag-number*

default ip route arp-to-host tag *tag-number*

Parameter Description

tag-number: Tag attribute value of the host route converted by ARP. The value range is from 1 to 4294967295, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the tag attribute value is configured for the host route converted by ARP, the route map can match the tag attribute to implement route control.

Examples

The following example configures the tag attribute of the host route converted by ARP.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip route arp-to-host tag 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip route notify delete always

Function

Run the **ip route notify delete always** command to configure direct deletion of the Border Gateway Protocol (BGP) route during graceful restart (GR).

Run the **no** form of this command to disable direct deletion of the BGP route during GR.

Run the **default** form of this command to restore the default configuration.

Direct deletion of the BGP route during GR is disabled by default.

Syntax

ip route notify delete always

no ip route notify delete always

default ip route notify delete always

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the function is enabled, the BGP route deletion configuration takes effect immediately during GR to prevent routing black hole.

Examples

The following example configures direct deletion of the BGP route during GR.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip route notify delete always
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ip routing

Function

Run the **ip routing** command to enable the IP routing function of a device.

Run the **no** form of this command to disable the IP routing function.

Run the **default** form of this command to restore the default configuration.

The IP routing function is enabled by default.

Syntax

ip routing

no ip routing

default ip routing

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a device functions only as a bridge or VoIP gateway, the IP routing and forwarding function of the device is not required. In this case, the IP routing function of the device can be disabled.

After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To prevent this situation, the static

route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

Examples

The following example disables the IP routing function of the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip routing
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ipv6 recur-route fastswitch-nexthop

Function

Run the **ipv6 recur-route fastswitch-nexthop** command to enable fast convergence of recursive routing.

Run the **no** form of this command to disable fast convergence of recursive routing.

Run the **default** form of this command to restore the default configuration.

The fast convergence function of recursive routing is disabled by default.

Syntax

ipv6 recur-route fastswitch-nexthop

no ipv6 recur-route fastswitch-nexthop

default ipv6 **recur-route fastswitch-nexthop**

Parameter Description

N/A

Command Modes

Global configuration mode

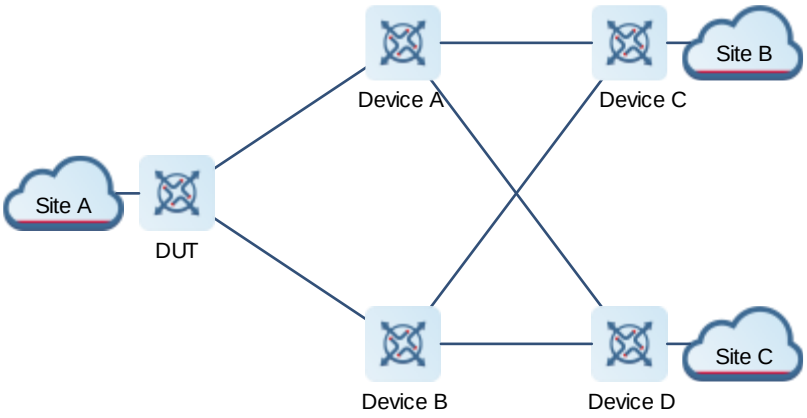
Default Level

14

Usage Guidelines

When link discovery changes or is interrupted, the recursive routing query of dynamic route may converge 2 seconds later. The convergence time is intolerable in some scenarios with high reliability requirements. When the fast convergence function of recursive routing is enabled, the intermediate next hop information will be added to the route sending information. Even if the intermediate link fails, it can be sensed by routing management to shorten the convergence time.

Figure 1-3 Fast Convergence Diagram of IPv6 Recursive Routing



As shown in Figure 1-3, the DUT establishes an IS-IS neighbor relationship with Device A and Device B respectively, Device A and Device B establish an IS-IS neighbor relationship with Device C and Device D respectively, and DUT establishes an IBGP neighbor relationship with Device C and Device D respectively. Service sites access the network via EBGP.

In the scenario shown above, BGP routes may be recursed to IS-IS routes. When the link between Device A and Device C is disconnected, the IS-IS route will change and the BGP route that relies on the IS-IS route needs to be re-calculated. Before the calculation result is delivered to the forwarding plane, the BGP traffic from Site A to Site B still goes through the disconnected link between Device A and Device C, resulting in traffic interruption. Traffic interruption duration = Link down time + Time required by the local IS-IS system to learn route deletion information + Time required by the local NSM system to receive IS-IS routing information + Time required for calculating the BGP route and delivering the result to the forwarding plane + Link switching time. The switching cannot be completed within 1 second.

If the fast convergence function of recursive routing is enabled, the traffic that needs to go through the disconnected link between Device A and Device C can be switched to a normal link within 1 second.

Examples

The following example enables the fast convergence function of recursive routing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 recur-route fastswitch-nexthop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 route nd-to-route delay-time

Function

Run the **ipv6 route nd-to-route delay-time** command to configure delayed redistribution of the routes converted by neighbor discovery (ND).

Run the **no** form of this command to delete delayed redistribution of the routes converted by ND.

Run the **default** form of this command to restore the default configuration.

The delayed redistribution function of the routes converted by ND is disabled by default. The delayed redistribution time is 0 seconds.

Syntax

ipv6 route nd-to-route delay-time

no ipv6 route nd-to-route delay-time

default ipv6 route nd-to-route delay-time

Parameter Description

delay-timetime: Delayed redistribution time of the routes converted by ND, in seconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To prevent route jitter caused by change to an ND entry, you can delay conversion of the ND entry into a route. After delayed redistribution is configured, redistribution of a route with effective ND will be delayed according to the specified delay time. For a route with invalid ND, advertising of the redistribution withdrawal route is not controlled, and the route will be advertised immediately.

Examples

The following example configures redistribution of the routes converted by ND to the protocol module after a delay of 10 seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 route nd-to-route delay-time 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 route nd-to-route interface

Function

Run the **ipv6 route nd-to-route interface** command to enable ND conversion to a route with fixed-length mask on the specified interface.

Run the **no** form of this command to disable ND-to-route conversion on the specified interface.

Run the **default** form of this command to restore the default configuration.

The ND-to-route conversion function is disabled on a specified interface by default.

Syntax

ipv6 route nd-to-route interface *interface-type interface-number* [**ipv6-prefix** *X:X:X:X::X/<0-128>*] [**prefix-len** *masklen*]

no ipv6 route nd-to-route interface *interface-type interface-number* [**ipv6-prefix** *X:X:X:X::X/<0-128>*] [**prefix-len**]

default ipv6 route nd-to-route interface *interface-type interface-number* [**ipv6-prefix** *X:X:X:X::X/<0-128>*] [**prefix-len**]

Parameter Description

interface-type interface-number: Interface name.

X:X:X:X::X/<0-128>: IPv6 network segment. If the ND entries match this network segment, the route is converted according to the mask specified by this network segment. If the network segment does not specify any mask, the default mask is **128**.

masklen: Mask length value of the ND-to-route. If an IPv6 network segment is specified, it is longer than the mask length of configured network segment. If no IPv6 network segment is specified, it is longer than the mask length of IPv6 address on the interface. Otherwise, the configuration fails. The value range is from 0 to 128, and the default value is **128**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Note

When configuring this command, make sure that the interface is a Layer-3 interface.

Parameter configuration rules:

- If neither the IPv6 network segment nor the IPv6 prefix is specified, the ND learned on the interface generates a 128-bit route by default.
- If no IPv6 network segment is specified and only IPv6 prefix is specified, all NDs on the interface generate the specified IPv6 prefix.
- If the IPv6 network segment is specified but no IPv6 prefix is specified, this network segment generates a 128-bit route by default.
- If both the network segment and IPv6 prefix are specified, when ND is learned, the prefix will be checked to find out the network segment it matches, and the configured IPv6 prefix is generated after the specified network segment matched is found.
- If both the network segment and IPv6 prefix are specified and the IPv6 prefix of an unspecified network segment is configured at the same time, a route will be generated according to the IPv6 prefix of the network segment if the network segment is matched, and a route will be generated according to the IPv6 prefix without network segment if the network segment is not matched.
- If you configure the IPv6 address of an interface before configuring the IPv6 prefix for the network segment of this interface address to generate a route with fixed-length mask, a configuration error occurs when the prefix-len is shorter than or equal to the mask of the IPv6 address. In addition, the IPv6 prefix command for the network segment of this interface address fails. For example, if you first configure IPv6 address 10::1/64 on the interface of VLAN 40, and then configure **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** in global configuration mode, the configuration fails.
- If you configure the IPv6 address of an interface before configuring the IPv6 prefix of an unspecified network segment, a configuration error occurs when the IPv6 prefix length is shorter than or equal to the mask length of any of the IPv6 addresses on the interface. In addition, the IPv6 prefix configuration command for the unspecified network segment fails. For example, if you first configure IPv6 address 10::1/64 on the interface of VLAN 40, and then configure **ipv6 route nd-to-route interface vlan 40 prefix-len 60** in global configuration mode, the configuration fails.
- If you configure the IPv6 prefix of an unspecified network segment before configuring the IPv6 address of this interface, syslog is displayed and the IPv6 prefix configuration of the unspecified network segment is canceled when the mask length of one of the IPv6 addresses is longer than or equal to the IPv6 prefix of the unspecified network segment. For example, if you first configure **ipv6 route nd-to-route interface vlan 40 prefix-len 60** in global configuration mode, and then configure address 10::1/64 on the interface of VLAN 40, syslog alarm is displayed and the configuration **ipv6 route nd-to-route interface vlan 40 prefix-len 60** is deleted.
- If you configure the IPv6 prefix of the specified network segment and then configure the IPv6 address of the corresponding network segment of the interface, syslog is displayed and the IPv6 prefix configuration of the

specified network segment is canceled when the IPv6 address mask of the corresponding network segment is longer than or equal to the IPv6 prefix of the specified network segment. For example, if you first configure **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** in global configuration mode, and then configure the address 10::1/64 on the interface of VLAN 40, the syslog alarm is displayed and the configuration **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** is deleted.

- If you configure the IPv6 prefix of an unspecified network segment and the IPv6 prefix of the specified network segment, and then configure the IPv6 address of the interface, please check whether the mask of each IPv6 address is longer than or equal to the IPv6 prefix of the specified/unspecified network segment. If so, syslog is displayed and the IPv6 prefix configuration of the corresponding network segment is canceled. For example, if you first configure **ipv6 route nd-to-route interface vlan 40 prefix-len 62** and **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** in global configuration mode, and then configure address 10::1/64 on the interface of VLAN 40, the syslog alarm is displayed and two configurations are deleted.

Examples

The following example enables ND-to-route conversion on the specified interface of VLAN 40 so that the ND matching the 10::1/58 network segment is converted to a route with a mask length of 110 bits, the ND matched to the 20::1/56 network segment is converted to a route with a mask length of 128 bits, and the remaining NDs are converted to routes with a mask length of 120 bits.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 route nd-to-route interface vlan 40 prefix-len 120
Hostname(config)# ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58
prefix-len 110
Hostname(config)# ipv6 route nd-to-route interface vlan 40 ipv6-prefix 20::1/56
prefix-len 128
```

Notifications

N/A

Common Errors

If the Layer-3 interface is not up, this function is unavailable.

Platform Description

N/A

Related Commands

N/A

1.12 ipv6 route nd-to-route tag

Function

Run the **ipv6 route nd-to-route tag** command to configure the tag attribute of the ND-converted route.

Run the **no** form of this command to delete the tag attribute of the ND-converted route.

Run the **default** form of this command to restore the default configuration.

The tag attribute function of the ND-converted route is disabled by default.

Syntax

ipv6 route nd-to-route tag *tag-number*

no ipv6 route nd-to-route

default ipv6 route nd-to-route tag

Parameter Description

tag-number: Tag attribute value of the ND-converted route. The value range is from 1 to 4294967295, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the tag attribute value is configured for the host route converted by ND, the route map can match the tag attribute to implement route control.

Examples

The following example sets the tag attribute of the ND-converted route to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 route nd-to-route tag 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv6 route nd-to-route warning-ignore

Function

Run the **ipv6 route nd-to-route warning-ignore** command to configure the function of ignoring warning log of ND conversion to a route of specified length.

Run the **no** form of this command to delete the function of ignoring warning log of ND conversion to a route of specified length.

Run the **default** form of this command to restore the default configuration.

The function of ignoring warning log of ND conversion to a route of specified length is disabled by default.

Syntax

ipv6 route nd-to-route warning-ignore

no ipv6 route nd-to-route warning-ignore

default ipv6 route nd-to-route warning-ignore

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After you configure the function of ignoring warning log of ND conversion to a route of specified length, the alarm that the same PORT ND generates the same network segment route is ignored. If this command is not configured, the warning log that the same Port ND generates the same network segment route is printed (only once). The alarm that different ports generate the same network segment route is not controlled by this command.

Examples

The following example configures the function of ignoring warning log of ND conversion to a route of specified length.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 route nd-to-route warning-ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 unicast-routing

Function

Run the **ipv6 unicast-routing** command to enable the IPv6 routing function of a device.

Run the **no** form of this command to disable the IPv6 routing function.

Run the **default** form of this command to restore the default configuration.

The IPv6 routing function is enabled by default.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

default ipv6 unicast-routing

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a device functions only as a bridge or VoIP gateway, the IPv6 routing and forwarding function of the device is not required. In this case, the IPv6 routing function of the device can be disabled.

Examples

The following example disables the IPv6 routing function of the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ipv6 unicast-routing
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 maximum-paths

Function

Run the **maximum-paths** command to configure the number of equal-cost routes.

Run the **no** form of this command to configure the default number of equal-cost routes.

Run the **default** form of this command to restore the default configuration.

32 equal-cost routes can be configured by default.

Syntax

maximum-paths *path-number*

no maximum-paths

default maximum-paths

Parameter Description

path-number: Number of equal-cost routes. The value range is from 1 to 32.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the number of equal-cost routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured equal-cost routes. You can run the **show running config** command to display the number of configured equal-cost routes.

This command is valid for both IPv4 and IPv6 addresses. After this command is configured, the maximum number of equal-cost routes to an IPv4 or IPv6 destination is equal to the configured value.

Examples

The following example sets the maximum number of equal-cost routes to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# maximum-paths 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route**

1.16 show ip route

Function

Run the **show ip route** command to display IP routing table information, as well as the equal-cost multi-path routing (ECMP) attribute of routes.

Syntax

show ip route [[**vr**f vrf-name] [**arphost** | **aggregate** | **count** | [**ecmp** | **fast-reroute** | **normal**] [*network* [*mask*]] | *network* [*mask* [**longer-prefix**]] | *route-protocol* [*process-id*] | **weight** | **tag**]

Parameter Description

vrf *vrf-name*: Displays the routing information only of the specified VRF. The routing information of global VRFs is displayed by default.

arphost: Displays the routing information of ARP conversion.

network: Target network to which the routing information is displayed. If no routing information of the target network is matched, the default route will be displayed. All routes are displayed by default.

mask: Mask whose target network routing information is displayed. The route matching the longest matching rule is displayed by default.

longer-prefix: Displays all the detailed routes matched with the specified prefix range.

count: Displays the number of current routes (the ECMP/WCMP route is calculated as one route). The statistics of the number of routes are not displayed by default.

route-protocol: Routing protocol or keywords: **connected**, **static**; to display a specific protocol route, use the following keywords: **bgp**, **isis**, **ospf**, **rip.** All protocols are displayed by default.

process-id: Routing protocol process ID. All the processes are displayed by default.

weight: Displays only routes with non-default weight. The routes of all weights are displayed by default.

normal: Displays normal routes, but not equal-cost routes and fast re-routes. All types of routes are displayed by default.

ecmp: Displays only equal-cost routes. All types of routes are displayed by default.

fast-reroute: Displays the primary/backup route of fast re-route only. All types of routes are displayed by default.

tag: Displays only routes of non-default tag. The routes of all tags are displayed by default.

aggregate: Displays only routes with type set to aggregated route. All types of routes are displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The command can be used to flexibly display the specified routing information according to the options.

The **show ip route** command is used to display the actual table entries that can be used for forwarding. To display the table entries of different attributes, specify the **normal** | **ecmp** | **fast-reroute** parameter.

Examples

The following example displays the IP routing table information, as well as the ECMP attribute of routes.

```
Hostname> enable
Hostname# show ip route
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
LA - Local aggregate route
       * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
LA   1.1.1.0/24 [1/0] via 0.0.0.0, Null 0
```

The following example displays normal routes, but not equal-cost routes and fast re-routes.

```
Hostname> enable
Hostname# show ip route normal
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host
```

The following example displays equal-cost routes.

```
Hostname> enable
Hostname# show ip route ecmp
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 192.168.1.2
            [1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
                     [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

The following example displays the primary/backup route of fast re-route.

```
Hostname> enable
Hostname# show ip route fast-reroute
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Status codes: m - main entry, b - backup entry, a – active entry
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [ma] via 192.168.1.2
            [b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
                 [ba] via 35.1.30.2, 00:38:26, VLAN 3
```

Table 1-1 Output Fields of the show ip route Command

Field	Description
O	Indicates the source routing protocol of the route. Value options of the field: **C**: Indicates direct route. **L**: Indicates local route. **S**: Indicates static route. **R**: Indicates RIP route. **B**: Indicates BGP route. **O**: Indicates OSPF route. **I**: Indicates IS-IS route.

Field	Description
E2	Indicates route type. Value options of the field: **E1**: Indicates OSPF external route type 1. **E2**: Indicates OSPF external route type 2. **N1**: Indicates OSPF NSSA external route type 1. **N2**: Indicates OSPF NSSA external route type 2. **SU**: Indicates IS-IS summary route. **L1**: Indicates IS-IS Level-1 route. **L2**: Indicates IS-IS Level-2 route. **IA**: Indicates internal route of routing domain.
20.0.0.0/8	Indicates the network address and mask length of the destination network.
[1/0]	Indicates the management distance/metric.
Via 20.0.0.1	Indicates the next-hop IP address.
00:00:06	Indicates the time to live (TTL) of protocol routing.
VLAN 1	Indicates the next-hop forwarding interface.

The following example displays the information of routing to the target network 30.0.0.0.

```
Hostname> enable
Hostname# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Table 1-2 Output Fields of the show ip route 30.0.0.0 Command

Field	Description
Distance	**Indicates the route management distance.**
metric	**Indicates the metric of the route.**
Routing Descriptor Blocks	Displays the next-hop IP address, routing source, update time, interface passed by, source routing protocol, type, BGP community attribute value of routing information.
00:01:11 ago	Indicates the TTL of protocol routing.
extern 2	Indicates the route type of source routing protocol of the route.

The following example displays the number of current routes.

```
Hostname> enable
```

```
Hostname# show ip route count
--- route info ---
the num of active route: 5(include ecmp: 9)
```

Table 1-3 Output Fields of the show ip route count Command

Field	Description
the num of active route	**Indicates the total number of currently active routes.**
include ecmp	**Indicates the number of ECMPs in the total routes.**

The following example displays routes of non-default weight.

```
Hostname> enable
Hostname# show ip route weight
----[distance/metric/weight]----
S    23.0.0.0/8 [1/0/2] via 192.1.1.20
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

Table 1-4 Output Fields of the show ip route weight Command

Field	Description
S	**Indicates the source routing protocol of the route.**
distance	**Indicates the route management distance.**
metric	**Indicates the metric of the route.**
weight	**Indicates the weight value of the route.**

The following example displays the primary/backup route of fast re-route to 30.0.0.0.

```
Hostname> enable
Hostname# show ip route fast-reroute 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
[ba]192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Table 1-5 Output Fields of the show ip route fast-reroute 30.0.0.0 Command

Field	Description
Distance	**Indicates the route management distance.**
metric	**Indicates the metric of the route.**
Routing Descriptor Blocks	Displays the next-hop IP address, routing source, update time, interface passed by, source routing protocol, type, BGP community attribute value of routing information.

Field	Description
[m]	Identifies the primary route.
[ba]	Identifies the backup route.
00:01:11 ago	Indicates the TTL of protocol routing.
extern 2	Indicates the route type of source routing protocol of the route.

The following example displays routes of non-default tag.

```
Hostname# show ip route tag
----[distance/metric/tag]----
S    23.0.0.0/8 [1/0/10] via 192.1.1.20
S    172.0.0.0/16 [1/0/20] via 192.0.0.1
```

Table 1-6 Output Fields of the show ip route tag Command

Field	Description
S	**Indicates the source routing protocol of the route.**
distance	**Indicates the route management distance.**
metric	**Indicates the metric of the route.**
tag	**Indicates the label value of the route.**

The following example displays aggregated routes.

```
Hostname(config)#show ip rou aggregate
LA    20.0.0.0/8 [1/0] via 0.0.0.0, Null 0
LA    21.0.0.0/8 [1/0] via 0.0.0.0, Null 0
```

Table 1-7 Output Fields of the show ip route aggregate Command

Field	Description
LA	Indicates a local aggregated route.

Notifications

N/A

Platform Description

N/A

1.17 show ip route recursive

Function

Run the **show ip route recursive** command to display the recursive information of an IP route.

Syntax

show ip route [[**vrf** *vrf-name*] **recursive** *ipv4-network/mask-length*

Parameter Description

vrf *vrf-name*: Displays the routing information only of the specified VRF. The routing information of global VRFs is displayed by default.

network/mask-length: Network address/length of subnet mask.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can display the detailed recursive information of an IP route, that is, all the routes that the IP route can be recursed to are listed according to the longest matching principle.

Examples

The following example displays the recursive information of an IP route.

```
Hostname> enable
Hostname# show ip route recursive 50.1.1.1/32
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, * - candidate default
S    50.1.1.1/32 [1/0] via 50.1.3.2
O IA  50.1.1.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
S*    0.0.0.0/0 is directly connected, Null 0
```

Table 1-8 Output Fields of the show ip route recursive Command

Field	Description
O	Indicates the source routing protocol of the route. Value options of the field: **C**: Indicates direct route. **L**: Indicates local route. **S**: Indicates static route. **R**: Indicates RIP route. **B**: Indicates BGP route. **O**: Indicates OSPF route. **I**: Indicates IS-IS route.
E2	Indicates route type. Value options of the field: **E1**: Indicates OSPF external route type 1. **E2**: Indicates OSPF external route type 2. **N1**: Indicates OSPF NSSA external route type 1. **N2**: Indicates OSPF NSSA external route type 2. **SU**: Indicates IS-IS summary route. **L1**: Indicates IS-IS Level-1 route. **L2**: Indicates IS-IS Level-2 route. **IA**: Indicates internal route of routing domain.
50.1.1.1/32	Indicates the network address and mask length of the destination network.
[1/0]	Indicates the management distance/metric.
50.1.3.2	Indicates the next-hop IP address.
00:38:26	Indicates the TTL of protocol routing.
VLAN 1	Indicates the next-hop forwarding interface.
Blocks	Displays the next-hop IP address, routing source, update time, interface passed by, source routing protocol, type, BGP community attribute value of routing information.

Notifications

N/A

Platform Description

N/A

1.18 show ip route static bfd

Function

Run the **show ip route static bfd** command to display the BFD correlation information of an IP route.

Syntax

show ip route [**vrf** *vrf-name*] **static bfd**

Parameter Description

vrf *vrf-name*: Displays the routing information only of the specified VRF. The routing information of global VRFs is displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can display the BFD correlation information of an IP route.

Examples

The following example displays the BFD correlation information of an IP route.

```
Hostname> enable
Hostname# show ip route static bfd
S    10.0.0.0/8 via 100.100.100.25, GigabitEthernet 0/3, BFD state is Up
S    20.0.0.0/8 via 200.100.100.25, GigabitEthernet 0/4, BFD state is Admin
```

Table 1-9 Output Fields of the show ip route static bfd Command

Field	Description
S	Indicates static route.
BFD state	Indicates the associated BFD state of static route.

Notifications

N/A

Platform Description

N/A

1.19 show ip route summary

Function

Run the **show ip route summary** command to display the statistics of a single routing table.

Run the **show ip route summary all** command to display the statistics of all the routing tables.

Syntax

show ip route [**vrf** *vrf-name*] **summary**

show ip route summary all

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF where this command is executed. If VRF is not specified, the command is executed on all VRFs.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the statistics of routing tables.

Examples

The following example displays the statistics of a single routing table.

```
Hostname> enable
Hostname# show ip route summary
Codes:  NORMAL – Normal route  ECMP – ECMP route  FRR – Fast-Reroute route
   Memory: 2000 bytes
Entries: 22, based on route prefixes
Entries: 29, based on route nexthops
: : :   NORMAL  ECMP    FRR     TOTAL
: Connected   3       0       0       3
: Static      2       1       1       4
: RIP         1       2       1       4
: OSPF        2       1       1       4
: ISIS        1       2       0       3
: BGP         2       1       1       4
: TOTAL       11      7       4       22
```

The following example displays the statistics of all the routing tables.

```
Hostname> enable
Hostname# show ip route summary all
Codes: NORMAL – Normal route  ECMP – ECMP route  FRR – Fast-Reroute route
IP routing table count:2
Total
Memory: 4000 bytes
Entries: 44, based on route prefixes
   Entries: 44,  based on route nexthops
: : :   NORMAL  ECMP    FRR     TOTAL
: Connected   6       0       0       6
```

```
: Static     4      2      2      8
: RIP        2      4      2      8
: OSPF       4      2      2      8
: ISIS       2      4      0      6
: BGP        4      2      2      8
: TOTAL      22     14     8      44
Global
Memory: 2000 bytes
Entries: 22, based on route prefixes
    Entries: 29, based on route nexthops
: : :   NORMAL  ECMP    FRR    TOTAL
: Connected   3      0      0      3
: Static     2      1      1      4
: RIP        1      2      1      4
: OSPF       2      1      1      4
: ISIS       1      2      0      3
: BGP        2      1      1      4
: TOTAL      11     7      4      22
VRF1
   Memory: 2000 bytes
Entries: 22, based on route prefixes
    Entries: 29, based on route nexthops
: : :   NORMAL  ECMP    FRR    TOTAL
: Connected   3      0      0      3
: Static     2      1      1      4
: RIP        1      2      1      4
: OSPF       2      1      1      4
: ISIS       1      2      0      3
: BGP        2      1      1      4
: TOTAL      11     7      4      22
```

Table 1-10 Output Fields of the show ip route summary Command

Field	Description
NORMAL	Indicates the classified entry type. Value options of the field: ● **NORMAL**: Indicates normal routing table entry (non-ECMP or FRR routing). ● **ECMP**: Indicates equal-cost multi-path routing table entry. ● **FRR**: Indicates fast re-route table entry. ● **TOTAL**: Indicates total of table entries of all types.
Memory	Indicates the size of the memory occupied by the current routing table.
Entries: x, based on route prefixes	Indicates the table entries contained in the current routing table (based on the prefix entries of table entries, not next hop entries)

Field	Description
Entries: x, based on route nexthops	Indicates the table entries contained in the current routing table (based on the next hop entries of table entries)
Connected	Indicates the protocol type of the table entry in this line. Value options of the field: **Connected**: Indicates table entries of direct route. **Static**: Indicates table entries of static route. **RIP**: Indicates table entries of RIP route. **OSPF**: Indicates table entries of OSPF route. **ISIS**: Indicates table entries of IS-IS route. **BGP**: Indicates table entries of BGP route. **TOTAL**: Indicates total of table entries in all protocols.
IP routing table count	Indicates the number of routing tables.
Global	Indicates the name of the current routing table. Value options of the field: **Global**: Indicates global (default VRF). **VRF1**: Indicates VRF name. **TOTAL**: Indicates total information of all the VRF routing tables.

Notifications

N/A

Platform Description

N/A

1.20 show ip route track-table

Function

Run the **show ip route track-table** command to display the track correlation information of an IP route.

Syntax

show ip route [**vrf** *vrf-name*] **track-table**

Parameter Description

vrf *vrf-name*: Displays the routing information only of the specified VRF. The routing information of global VRFs is displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can display the track correlation information of an IP route.

Examples

The following example displays the track correlation information of an IP route.

```
Hostname> enable
Hostname# show ip route track-table
ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]
ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0 2 track 3 state is [down]
```

Table 1-11 Output Fields of the show ip route track-table Command

Field	Description
track	Indicates the track object index.
state	Indicates the track object state.

Notifications

N/A

Platform Description

N/A

1.21 show ipv6 route

Function

Run the **show ipv6 route** command to display the routing information of an IPv6 route.

Syntax

show ipv6 route [[**vrf** *vrf-name*] [[**fast-reroute**] *ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *route-protocol* [*process-id*] | **weight**]]

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF where this command is executed. If VRF is not specified, the command is executed on all VRFs.

fast-reroute: Displays the primary/backup route of fast re-route only. All types of routes are displayed by default.

ipv6-prefix/*prefix-length*: Specified prefix of the IPv6 route to be exactly matched. All the routes are displayed by default.

longer-prefixes: Displays the longest IPv6 route that matches the specified prefix. All the routes are displayed by default.

route-protocol: Routing protocol or keywords: **connected**, **local, static**; to display a specific protocol route, use the following keywords: **bgp**, **isis**, **ospf**, **rip.** The routes of all protocols are displayed by default.

process-id: Routing protocol process ID. The routes of all the processes are displayed by default.

weight: Displays only routes with non-default weight. The routes of all weights are displayed by default.

tag: Displays only routes of non-default tag. The routes of all tags are displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the information of IPv6 routing tables.

Examples

The following example displays the routing information of IPv6.

```
Hostname> enable
Hostname# show ipv6 route
IPv6 routing table - Default - 7 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area
C      10::/64  via Loopback 1, directly connected
L      10::1/128  via Loopback 1, local host
S      20::/64 [20/0] via 10::4, Loopback 1C
C      FE80::/10 via Null 0, directly connected
C      FE80::/64  via Loopback 1, directly connected
L      FE80::2D0:F8FF:FE22:33AB/128  via Loopback 1, local host
```

Table 1-12 Output Fields of the show ipv6 route Command

Field	Description
S	Indicates the source routing protocol of the route. Value options of the field: **C**: Indicates direct route. **L**: Indicates local route. **S**: Indicates static route. **R**: Indicates RIP route. **B**: Indicates BGP route. **O**: Indicates OSPF route. **I**: Indicates IS-IS route.

Field	Description
E2	Indicates route type. Value options of the field: **E1**: Indicates OSPF external route type 1. **E2**: Indicates OSPF external route type 2. **N1**: Indicates OSPF NSSA external route type 1. **N2**: Indicates OSPF NSSA external route type 2. **SU**: Indicates IS-IS summary route. **L1**: Indicates IS-IS Level-1 route. **L2**: Indicates IS-IS Level-2 route. **IA**: Indicates internal route of routing domain.
20::/64	Indicates the network address and mask length of the destination network.
[20/0]	Indicates the management distance/metric.
via 10::4	Indicates the next-hop IPv6 address.
Loopback 1	Indicates the next-hop forwarding interface.

Notifications

N/A

Platform Description

N/A

1.22 show ipv6 route static bfd

Function

Run the **show ipv6 route static bfd** command to display the BFD correlation information of an IPv6 route.

Syntax

show ipv6 route [**vrf** *vrf-name*] **static bfd**

Parameter Description

vrf *vrf-name*: Displays the routing information of the specified VRF only. The routing information of global VRFs is displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can display the BFD correlation information of an IPv6 route.

Examples

The following example displays the BFD correlation information of an IPv6 route.

```
Hostname> enable
Hostname# show ip route static bfd
S    25::/64 via 100::25, GigabitEthernet 0/3, BFD state is Up
S    26::/64 via 200::25, GigabitEthernet 0/4, BFD state is Admin
```

Table 1-13 Output Fields of the show ip route static bfd Command

Field	Description
S	Indicates static route.
BFD state	Indicates the associated BFD state of static route.

Notifications

N/A

Platform Description

N/A

1.23 show ipv6 route summary

Function

Run the **show ipv6 route summary** command to display the statistics of a single IPv6 routing table.

Run the **show ipv6 route summary all** command to display the statistics of all the IPv6 routing tables.

Syntax

show ipv6 route [**vrf** *vrf-name*] **summary**

show ipv6 **route summary all**

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF where this command is executed. If VRF is not specified, the command is executed on all VRFs.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the statistics of IPv6 routing tables.

Examples

The following example displays the statistics of a single IPv6 routing table.

```
Hostname> enable
Hostname# show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local         2
Connected      3
Static         0
RIP           0
OSPF          0
BGP           0
Total          5
```

The following example displays the statistics of all the IPv6 routing tables.

```
Hostname> enable
Hostname# show ipv6 route summary all
IPv6 routing table count: 2
Total
  Memory: 2000 bytes
  Entries: 20
    Local:2,Connected:2,Static:8,RIP:2,OSPF:2,ISIS:2,BGP:2
Global
  Memory: 1000 bytes
  Entries: 10
Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS:1,BGP:1
VRF1
  Memory: 1000 bytes
  Entries: 10
Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS:1,BGP:1
```

Table 1-14 Output Fields of the show ipv6 route summary Command

Field	Description
Memory	Indicates the size of the memory occupied by the current routing table.
Entries	Indicates the table entries contained in the current routing table (based on the prefix entries of table entries, not next hop entries)

Field	Description
Connected	Indicates the protocol type of the table entry in this line. Value options of the field: **Connected**: Indicates table entries of direct route. **Static**: Indicates table entries of static route. **RIP**: Indicates table entries of RIP route. **OSPF**: Indicates table entries of OSPF route. **ISIS**: Indicates table entries of IS-IS route. **BGP**: Indicates table entries of BGP route. **TOTAL**: Indicates total of table entries in all protocols.
IPv6 routing table count	Indicates the number of routing tables.
Global	Indicates the name of the current routing table. Value options of the field: **Global**: Indicates global (default VRF). **VRF1**: Indicates VRF name. **TOTAL**: Indicates total information of all the VRF routing tables.

Notifications

N/A

Platform Description

N/A

1.24 show route-res usage

Function

Run the **show route-res usage** command to display the usage of routing resources.

Syntax

show route-res usage [**all** | **slot** *slot-id*]

Parameter Description

all: Displays the routing information of all the slots.

slot *slot-id*: Specifies the slot for viewing routing resource information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The command is used to display the routing resource information of the specified slot.

Examples

The following example displays the usage of routing resources of all the slots.

```
Hostname> enable
Hostname# show route-res usage all
Switch  Slot    Switch Mode Current:
-------------------------------------------------------------------------------
1       0       default
-------------------------------------------------------------------------------
L3 Software Statistics:
-----------------------
Switch  Slot    Chip    Name           Used    Description
-------------------------------------------------------------------------------
1       0       0       IPv4_LPM       1       ipv4 route in lpm table
1       0       0       IPv4_HOST      0       ipv4 route in l3_entry table

1       0       0       IPv6_64_LPM    0       ipv6-64 route in lpm table
1       0       0       IPv6_128_LPM   0       ipv6-65-128 route in lpm table
1       0       0       IPv6_HOST      0       ipv6 route in l3_entry table
-------------------------------------------------------------------------------
Switch  Slot    Chip    Name           Used    Max     Description
-------------------------------------------------------------------------------
1       0       0       NEXTHOP        1       18432   nexthop number
1       0       0       ECMP_GROUP     0       75      ecmp group number
1       0       0       ENCAP          0       0       encap number

L3 Forwarding Statistics:
-------------------------
Switch  Slot    Chip    Resource     Service      Max       Used[   %]     Remain
```

Table 1-15 Output Fields of the show route-res usage Command

Field	Description
Switch	Indicates device ID.
Slot	Indicates slot ID.
Switch Mode Current	Indicates the current UFT mode.
Chip	Indicates the switching chip ID.
Name	Indicates the entry name.
Used	Indicates the used quantity.

Field	Description
Description	Indicates the description information.
Max.	Indicates the maximum value.
Resource	Indicates the resource name.
Remain	Indicates the remaining capacity.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 Static Route Commands

Command	Function
clear ip route arp scan times	Clear the Address Resolution Protocol (ARP) request transmission count and start counting again.
ip default-gateway	Configure a default gateway.
ip default-network	Configure a default network.
ip fast-reroute static route-map	Enable static fast reroute.
ip route	Configure static route.
ip route scan arp interval	Set the interval for actively sending ARP requests when ARP fails after correlation of static routes with ARP is configured.
ip route scan arp times	Set the times of actively sending ARP requests when ARP fails after correlation of static routes with ARP is configured.
ip route static bfd	Configure correlation of static routes with BFD.
ip route static inter-vrf	Allow static routing across VRFs.
ip static route-limit	Configure the maximum number of static routes.
ipv6 default-gateway	Configure a default gateway on a Layer-2 device.
ipv6 fast-reroute static route-map	Enable static fast reroute.
ipv6 route	Configure IPv6 static route.
ipv6 route static bfd	Configure correlation of static routes with BFD.
ipv6 static route-limit	Configure the maximum number of static routes.
maximum routes	Limit the maximum number of routes in the default VRF.
show ip redirects	Display the default gateway.
show ipv6 redirects	Display the IPv6 default gateway.

1.1 clear ip route arp scan times

Function

Run the **clear ip route arp scan times** command to clear the Address Resolution Protocol (ARP) request transmission count and start counting again.

Syntax

clear ip route arp scan times

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

If the configured transmission count of ARP requests is 10 but no ARP reply is received after the ARP request has been sent 10 times, the device no longer sends the ARP request. If you need to continue to send the ARP request, run this command to clear the count so that the device can continue to actively send the ARP request.

Examples

The following example clears the transmission count of ARP request.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route scan arp times 10
Hostname(config)# exit
Hostname# clear ip route arp scan times
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip default-gateway

Function

Run the **ip default-gateway** command to configure a default gateway.

Run the **no** form of this command to delete the default gateway.

Run the **default** form of this command to restore the default configuration.

No default gateway is configured by default.

Syntax

ip default-gateway *ipv4-address*

no ip default-gateway

default ip default-gateway

Parameter Description

ipv4-address: Default gateway IPv4 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

During data interaction, the packet with a destination address not in the local network segment is sent to the default gateway, and the gateway completes the next-step routing, achieving internetworking between the device and other networks.

Examples

The following example configures the default gateway as 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip default-gateway 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

This command is supported after the **no ip routing** command is used on devices.

Related Commands

- **show ip redirects**

1.3 ip default-network

Function

Run the **ip default-network** command to configure a default network.

Run the **no** form of this command to delete a default network.

Run the **default** form of this command to restore the default configuration.

The network ID is 0.0.0.0/0 by default.

Syntax

ip default-network *network*

no ip default-network *network*

default ip default-network *network*

Parameter Description

network: Network ID of the default network.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Configuring a default network aims to generate a default route. To generate a default route using the **default-network** command, make sure that the default network is not a directly-connected interface network, but is reachable in the routing table.

The default network always starts with an asterisk (*), indicating that it is a candidate for the default route. If there are direct routes and routes without next hop on the default network, the default route must be a static route.

Examples

The following example configures the default network as 192.168.100.0. Since a static route to the network is configured, the device will automatically generate a default route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route 192.168.100.0 255.255.255.0 gigabitethernet 0/1
Hostname(config)# ip default-network 192.168.100.0
```

The following example configures the default network as 200.200.200.0. As long as 200.200.200.0 appears in the routing table, the route becomes a default route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip default-network 200.200.200.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP Routing Basic)

1.4 ip fast-reroute static route-map

Function

Run the **ip fast-reroute static route-map** command to enable static fast reroute.

Run the **no** form of this command to disable static fast reroute.

Run the **default** form of this command to restore the default configuration.

The static fast reroute function is disabled by default.

Syntax

ip fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

no ip fast-reroute [**vrf** *vrf-name*] **route-map**

default ip fast-reroute [**vrf** *vrf-name*] **route-map**

Parameter Description

vrf-name: Virtual routing and forwarding (VRF). If no VRF is specified, the command is executed on all VRFs.

route-map-name: Route map of static fast reroute.

static: Generates a backup route for the static route.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Fast reroute sends the primary link route and backup link route at the same time. When the primary link fails, packets can be directly switched to the backup link route for forwarding, reducing service interruption time. For static fast reroute, when the primary next hop fails, the backup next hop, if valid, becomes the primary next hop for forwarding.

To improve the switching performance of fast reroute, bidirectional forwarding detection (BFD) detection can be started for the next hop of primary link. If the interface is Up or Down, to shorten the forwarding interruption time

during fast reroute, you can configure **carrier-delay 0** in interface configuration mode of the primary link egress to achieve the fastest switching performance.

Examples

The following example enables static fast reroute, and sets the backup next hop of all static routes to 192.168.1.2 to forward packets through the Gigabit Ethernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map fast-reroute
Hostname(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1
192.168.1.2
Hostname(config-route-map)# exit
Hostname(config)# ip fast-reroute static route-map fast-reroute
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip route

Function

Run the **ip route** command to configure static route.

Run the **no** form of this command to delete the configured static route.

Run the **no ip route all** command to delete all the configured static routes.

Run the **default ip route** command to restore the default configuration.

Run the **default ip route all** command to restore the default configuration.

No static route is configured by default.

Syntax

ip route [**vrf** *vrf-name*] *network mask* { *ipv4-address* [**global**] | *interface* [*ipv4-address* [**arp** | **global**] *] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | [**track** *object-number*] [**permanent**] | **tag** *tag* | **weight** *number*] *

no ip route [**vrf** *vrf-name*] { **all** | *network mask* { *ipv4-address* | *interface* [*ipv4-address*] } [*distance*] }

default ip route [**vrf** *vrf-name*] { **all** | *network mask* { *ipv4-address* | *interface* [*ipv4-address*] } [*distance*] }

Parameter Description

vrf *vrf-name*: Specifies the route VRF, which can be a single-protocol IPv4 VRF or a multi-protocol VRF configured with an IPv4 address family. The VRF is a global VRF by default.

network: Address of the target network.

mask: Mask of the target network.

ipv4-address: Next hop address of the static route. You must specify at least one of *ipv4-address* and *interface*, or both. If *ipv4-address* is not specified, a static direct route is configured.

global: Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by *vrf-name*.

interface: Next-hop egress of the static route. You must specify at least one of *ipv4-address* and *interface*, or both. If *interface* is not specified, a recursive static route is configured. The egress is obtained by the next hop from the routing table.

arp: Creates routes according to ARP entries.

distance: Management distance of the static route. The value range is from 1 to 255, and the default value is **1**.

tag: Tag value of the static route. The value range is from 1 to 4294967295, and the default value is **0**.

permanent: Indicates a permanent route. The static route is not a permanent route by default.

track *object-number*: Indicates correlation with track. *object-number* indicates the ID of the track object. By default, the static route is not correlated with the track function.

weight *number*: Specifies the weight of the static route. The value range is from 1 to 8, and the default value is **1**.

description *description-text*: Specifies the static route description. By default, no description is configured. Here, *description-text* is a string of 1 to 60 characters.

disabled/enabled: Indicates the enable flag of the static route. The flag is **enabled** by default.**all**: Deletes all static routes under the specified VRF.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In a small network, you can configure IPv4 static routes to implement internetworking.

The management distance of the static route is 1 by default. Setting the management distance allows the routes learned by a dynamic routing protocol to cover static routes. The static route is used only when dynamic routes cannot be learned. Setting the management distance of a static route can implement line backup. In this case, the static route is also called floating route. For example, the management distance of Open Shortest Path First (OSPF) routing protocol is 110, and the management distance of static route can be set to 125. In this way, when the line running OSPF fails, the data traffic can be switched to the line of static route.

The VRF to which the static route belongs can be specified. If it is not specified, the static route will be added to the default VRF. If the specified VRF is a multi-protocol VRF, it must be configured with an IPv4 address family;

otherwise, static route cannot be configured. Deleting the IPv4 address family of a multi-protocol VRF will also delete the IPv4 static route of this VRF.

The default weight of a static route is 1. You can run the **show ip route weight** command to display static routes with non-default weight. The weight parameter **weight** is used to implement the Weighted Cost Multipath (WCMP) function. When load-balancing routes can reach an address, the network device will allocate data traffic according to the weight value of each route. The route with a larger **weight** will share more data packets, and the route with a smaller **weight** will share less data packets. The WCMP limit of the device is 32 generally. When the weight sum of load balancing routes is greater than the limit, the routes beyond the limit will not take effect.

The configuration flag of a static route controls whether the static route is valid. If it is invalid, it will not be used for forwarding. The persistent route is configured to the forwarding table. It will always exist unless it is deleted by the network administrator.

When you want to configure a static route through an Ethernet interface, avoid directly setting the next hop to an interface (such as **ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/0**) if possible. If the next hop is directly an interface, the device deems that all the unknown target networks are directly connected to the Gigabit Ethernet 0/0 interface. Then, it sends an ARP request to every target host, thus occupying a lot of CPU and memory resources. Therefore, you are not advised to directly point a static route to an Ethernet interface.

Correlation of a static route with a track can be specified. When correlation of a static route with a specified track object is configured and the advertised status of the track object is inactive, the static route does not take effect. If the advertised status of the track object is active, the static route takes effect based on another status. With correlation of a static route with a track object, the third-party status concerned by the track object is mainly used to determine whether the static route takes effect. Correlation of a static route with a track object cannot be used for routes with the permanent attribute.

Correlation of a static route with an ARP object can be specified. When correlation of a static route with an ARP object is configured and the ARP object corresponding to the next hop and egress of the route does not exist, the static route does not take effect. When the ARP object corresponding to the next hop and egress of the route exits, the static route takes effect based on another status. Correlation of a static route with an ARP object cannot be used for routes with the permanent attribute.

Correlation of a static route with a track object cannot be used together with correlation of a static route with an ARP object.

Examples

The following example configures a static route. The next hop to 172.16.100.0/24 is 192.168.12.1, and the management distance is 115.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route 172.16.100.0 255.255.255.0 192.168.12.1 115
```

The following example configures a static route. The next hop to 172.16.100.0/24 is 192.168.2.1, and data traffic can be forwarded only from the Gigabit Ethernet 0/0 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route 172.16.100.0 255.255.255.0 GigabitEthernet 0/1
192.168.12.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP Routing Basic)

1.6 ip route scan arp interval

Function

Run the **ip route scan arp interval** command to set the interval for actively sending ARP requests when ARP fails after correlation of static routes with ARP is configured.

Run the **no** form of this command to delete the configured interval for actively sending ARP requests and restore it to the default value.

Run the **default** form of this command to restore the default configuration.

The correlation of static routes with ARP is disabled by default, and the ARP request is sent every 5s.

Syntax

ip route scan arp interval *request-interval*

no ip route scan arp interval

default ip route scan arp interval

Parameter Description

request-interval: Interval for actively sending ARP requests, in seconds. The range is from 5 to 120.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the correlation of static routes with ARP is configured, when ARP fails due to a link failure or other causes, the device actively sends ARP requests. The transmission interval can be configured. By default, ARP requests are sent at an interval of 5s.

Examples

The following example configures correlation of static routes with ARP. When ARP fails, ARP requests are sent actively at an interval of 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route scan arp interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip route scan arp times

Function

Run the **ip route scan arp times** command to set the times of actively sending ARP requests when ARP fails after correlation of static routes with ARP is configured.

Run the **no** form of this command to delete the configured times of actively sending ARP requests and restore it to the default value.

Run the **default** form of this command to restore the default configuration.

By default, the correlation of static routes with ARP is disabled, and the ARP request is sent 65,535 times.

Syntax

ip route scan arp times *request-times*

no ip route scan arp times

default ip route scan arp times

Parameter Description

request-times: Times of actively sending ARP requests when the ARP fails. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After correlation of static routes with ARP is configured, when the ARP fails due to a link failure or other causes, the device actively sends ARP requests and the sending count can be configured. ARP requests are sent 65,535 times by default.

Examples

The following example configures correlation of static routes with ARP. When the ARP fails, the ARP request is actively sent 10 times.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip route scan arp times 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ip route static bfd

Function

Run the **ip route static bfd** command to configure correlation of static routes with BFD.

Run the **no** form of this command to delete the configured correlation of static routes with BFD.

Run the **default** form of this command to restore the default configuration.

Correlation of static routes with BFD is disabled by default.

Syntax

ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv4-address*]

no ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv4-address*]

default ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv4-address*]

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF to which the static device belongs. The VRF is a global VRF by default.

interface-type interface-number: Interface type and interface number.

gateway: Gateway IP address, which is the neighbor IP address of BFD. If the next hop of the static route is this neighbor, BFD is used to check the connectivity of the forwarding path.

source *ipv4-address*: Specifies the source IP address used for the BFD session. If the neighbor IP address involves multiple hops, this parameter must be configured. By default, the source IP address is not specified.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can use this function to configure correlation of IPv4 static routes with BFD, quickly sensing change to the destination address link. If the Down status of the BFD session is detected, the IPv4 static route is not active and does not participate in packet forwarding. Before configuration, make sure that the BFD session parameters are configured on the interface.

Examples

The following example enables correlation of static routes with BFD and detects the forwarding path to the neighbor 172.16.0.2 via BFD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no switchport
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.0.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# ip route static bfd GigabitEthernet 0/1 172.16.0.2
Hostname(config)# ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/1 172.16.0.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bfd interval** (reliability/BFD)

1.9 ip route static inter-vrf

Function

Run the **ip route static inter-vrf** command to allow static routing across VRFs.

Run the **no** form of this command to disable static routing across VRFs.

Run the **default** form of this command to restore the default configuration.

Static routing across VRFs is allowed by default.

Syntax

ip route static inter-vrf

no ip route static inter-vrf

default ip route static inter-vrf

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If you configure **no ip route static inter-vrf**, static routing across VRFs will not take effect. If active static routing across VRFs already exists and you configure it again, information similar to the following will be printed, instructing you to delete the static routing across VRFs.

```
*Aug 7 10:58:34: %NSM-ROUTESACROSSVRF: Un-installing route [x.x.x.x/8] from global routing table with outgoing interface x/x.
```

Examples

The following example prohibits static routing across VRFs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip route static inter-vrf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip static route-limit

Function

Run the **ip static route-limit** command to configure the maximum number of static routes.

Run the **no** form of this command to configure the default number of routes.

Run the **default** form of this command to restore the default configuration.

The configured maximum number of static routes is 1000 by default.

Syntax

ip static route-limit { *number* | **default-vrf** *number* | **vrf** *vrf-name number* }

no ip static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

default ip static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

Parameter Description

number: Maximum number of all the static routes of a device. The value range is from 1 to 1000000.

default-vrf *number*: Specifies the maximum number of static routes under the default VRF. The value range is from 1 to 10000.

vrf *vrf-name number*: Specifies the maximum number of static routes under the VRF. The value range is from 1 to 10000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the maximum number of static routes is configured using **ip static route-limit**, the number of static routes configured will not exceed the maximum number set. You can run the **show running-config** command to display the currently configured maximum number of non-default static routes.

Examples

The following example configures the maximum number of static routes as 9000, the maximum number of static routes of the default VRF as 2000, and the maximum number of static routes of VRF test as 1000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip static route-limit 9000
Hostname(config)# ip static route-limit default-vrf 2000
Hostname(config)# ip static route-limit vrf test 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 default-gateway

Function

Run the **ipv6 default-gateway** command to configure a default gateway on a Layer-2 device.

Run the **no** form of this command to delete the default gateway.

Run the **default** form of this command to restore the default configuration.

No IPv6 default gateway is configured by default.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

default ipv6 default-gateway

Parameter Description

ipv6-address: Default gateway IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

During data interaction, the packet with a destination address not in the local network segment is sent to the default gateway, and the gateway completes the next-step routing, achieving internetworking between the device and other networks. You can run the **show ipv6 redirects** command to display the default gateway configuration.

Examples

The following example configures the default IPv6 gateway as 10::1 on a Layer-2 device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 default-gateway 10::1
```

Notifications

N/A

Common Errors

N/A

Platform Description

This command is supported after the **no ipv6 unicast-routing** command is used on devices.

Related Commands

- **show ipv6 redirects**

1.12 ipv6 fast-reroute static route-map

Function

Run the **ipv6 fast-reroute static route-map** command to enable static fast reroute.

Run the **no** form of this command to disable static fast reroute.

Run the **default** form of this command to restore the default configuration.

The static fast reroute function is disabled by default.

Syntax

ipv6 fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

no ipv6 fast-reroute [**vrf** *vrf-name*]

default ipv6 fast-reroute [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Specifies the VRF name. If the VRF name is not specified, the command is executed on all VRFs.

route-map-name: Route map of static fast reroute.

static: Generates a backup route for the static route.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Fast reroute sends the primary link route and backup link route at the same time. When the primary link fails, packets can be directly switched to the backup link route for forwarding, reducing service interruption time.

To improve the switching performance of fast reroute, BFD detection can be enabled for the next hop of primary link. If the interface is Up or Down, to shorten the forwarding interruption time during fast reroute, you can configure **carrier-delay 0** in interface configuration mode of the primary link egress to achieve the fastest switching performance.

For static fast reroute, when the primary next hop fails, the backup next hop, if valid, becomes the primary next hop for forwarding.

Examples

The following example enables static fast reroute, and sets the backup next hop of all static routes to 2001::1 to forward packets through the Gigabit Ethernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map fast-reroute
Hostname(config-route-map)# set ipv6 fast-reroute backup-interface GigabitEthernet
0/1 backup-nexthop 2001::1
Hostname(config-route-map)# exit
```

```
Hostname(config)# ipv6 fast-reroute static route-map fast-reroute
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv6 route

Function

Run the **ipv6 route** command to configure IPv6 static route.

Run the **no** form of this command to delete the configured static route.

Run the **no ipv6 route all** command to delete all the configured static routes.

Run the **default ipv6 route** command to restore the default configuration.

Run the **default ipv6 route all** command to restore the default configuration.

The IPv6 static route function is disabled by default.

Syntax

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix* / *prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

no ipv6 route [**vrf** *vrf-name*] { **all** | *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] }

default ipv6 route [**vrf** *vrf-name*] { **all** | *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] }

Parameter Description

vrf *vrf-name*: Specifies the VRF to which the route belongs. This parameter must be a multi-protocol VRF with configured IPv6 address family. The VRF is a global VRF by default.

ipv6-prefix: IPv6 prefix, which must comply with the address representation format specified in RFC4291.

prefix-length: Length of the IPv6 prefix. A slash (/) must be added before the prefix.

ipv6-address: Next hop address of the static route. You must specify at least one of *ipv6-address* and *interface*, or both. If *ipv6-address* is not specified, a static direct route is configured.

interface: Next-hop egress of the static route. You must specify at least one of *ipv6-address* and *interface*, or both. If *interface* is not specified, a recursive static route is configured. The egress is obtained by the next hop from the routing table.

nexthop-vrf *vrf-name1*: Specifies the VRF to which the next hop belongs. This parameter must be a multi-protocol VRF with configured IPv6 address family. By default, the VRF of the next hop is the same as the VRF specified by the VRF name. Here, **nexthop-vrf default** indicates that the VRF of the next hop is a global VRF.

distance: Management distance of the static route. The management distance is 1 by default.

tag *tag*: Specifies the tag value of the static route. The value range is from 1 to 4294967295, and the default value is **0**.

weight *number*: Specifies the weight of the static route, which must be specified when you configure equal-cost routes. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The value range is from 1 to 8, and the default value is **1**.

description *description-text*: Specifies the static route description. By default, no description is configured. Here, *description-text* is a string of 1 to 60 characters.

all: Deletes all static IPv6 routes under the specified VRF.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

On a simple network, you can configure IPv6 static routes to implement internetworking.

Deleting the IPv6 address family of a multi-protocol VRF will also delete the IPv6 static routes in the VRF table or next-hop routes. If the VRF of the interface of an IPv6 static route is inconsistent with the configured VRF of the next hop, this IPv6 static route will not take effect.

The default management distance of static routes is 1. Setting the management distance allows the route learned by the dynamic route to cover the static route. Only when the dynamic route cannot be learned, can the static route be used. Setting the management distance of a static route can implement line backup. In this case, the static route is also called floating route. For example, the management distance of OSPF routing protocol is 110, and the management distance of static route can be set to 125. In this way, when the line running OSPF fails, the data traffic can be switched to the line of static route.

Examples

The following example configures an IPv6 static route. The target network of the traffic is 2001::/64, the next hop is 2002::2, and the management distance is 115.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 route 2001::/64 2002::2 115
```

The following example configures an IPv6 static route. The target network of the traffic is 2001::/64, the next hop is 2002::2, and data traffic can be forwarded only from the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 route 2001::/64 GigabitEthernet 0/1 2002::2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 route** (IP Routing Basic)

1.14 ipv6 route static bfd

Function

Run the **ipv6 route static bfd** command to configure correlation of static routes with BFD.

Run the **no** form of this command to delete the configured correlation of static routes with BFD.

Run the **default** form of this command to restore the default configuration.

Correlation of static routes with BFD is disabled by default.

Syntax

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

no ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

default ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF to which the static device belongs. If VRF is not specified, the command is executed on all VRFs.

interface-type interface-number: Interface type and interface number.

gateway: Gateway IP address, which is the neighbor IP address of BFD. If the next hop of the static route is this neighbor, BFD is used to check the connectivity of the forwarding path.

source *ipv6-address*: Specifies the source IP address used for the BFD session. If the neighbor IP address involves multiple hops, this parameter must be configured. By default, the neighbor IP address of the BFD session is a single hop, and the source IP address is not used.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can use this function to configure correlation of IPv6 static routes with BFD, quickly sensing change to the destination address link. If the Down status of the BFD session is detected, the IPv6 static route is not active and does not participate in packet forwarding. Before configuration, make sure that the BFD session parameters are configured on the interface.

Examples

The following example enables correlation of static routes with BFD and detects the forwarding path to the neighbor 2001:1::2 via BFD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if)# no switchport
Hostname(config-if)# ip address 2001:1::1/64
Hostname(config-if)# bfd interval 50 min_rx 50 multiplier 3
Hostname(config-if)#exit
Hostname(config)# ipv6 route static bfd GigabitEthernet 0/1 2001:1::2
Hostname(config)# ipv6 route 2002::/64 GigabitEthernet 0/1 2001:1::2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ipv6 static route-limit

Function

Run the **ipv6 static route-limit** command to configure the maximum number of static routes.

Run the **no** form of this command to configure the default number of routes.

Run the **default** form of this command to restore the default configuration.

The maximum number of static routes is 1000 by default.

Syntax

ipv6 static route-limit { *number* | **default-vrf** *number* | **vrf** *vrf-name number* }

no ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

default ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

Parameter Description

number: Maximum number of all the static routes of a device. The value range is from 1 to 1000000.

default-vrf *number*: Specifies the maximum number of static routes under the default VRF. The value range is from 1 to 10000.

vrf *vrf-name number*: Specifies the maximum number of static routes under the VRF. The value range is from 1 to 10000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the maximum number of static routes is configured using **ipv6 static route-limit**, the number of static routes configured will not exceed the maximum number set. You can run the **show running config** command to display the currently configured maximum number of non-default static routes.

Examples

The following example configures the maximum number of static routes in global IPv6 mode as 900, the maximum number of static routes of the default VRF as 200, and the maximum number of static routes of VRF test as 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 static route-limit 900
Hostname(config)# ipv6 static route-limit default-vrf 200
Hostname(config)# ipv6 static route-limit vrf test 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 maximum routes

Function

Run the **maximum routes** command to limit the maximum number of routes in the default VRF.

Run the **no** form of this command to cancel limitation to the maximum number of routes in the default VRF.

The maximum number of routes in the default VRF is not limited by default.

Syntax

maximum routes *limit* { *warn-threshold* | **warning-only** }

no maximum routes

Parameter Description

limit: Maximum number of routes. The routes beyond the limit are not written to the core routing table. The value range is from 1 to 4294967295.

warn-threshold: Threshold for printing warning. Warning will be printed when this percentage is reached. The value range is from 1 to 100.

warning-only: Only prints warning and still allows routes to be added to the core routing table when the configured maximum number is reached.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to limit the number of routes running in the default VRF. If you want warning only, use the **warning-only** parameter.

Examples

The following example configures the maximum number of routes under the default VRF as 1000. When the number of routes exceeds 1000*100%, the warning log will be given.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# maximum routes 1000 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP Routing Basic)

1.17 show ip redirects

Function

Run the **show ip redirects** command to display the default gateway.

Syntax

show ip redirects

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the gateway configuration of a device. This command can be used after the **no ip routing** command is used on devices.

Examples

The following example displays the default gateway.

```
Hostname> enable
Hostname# show ip redirects
Default Gateway: 192.168.195.1
```

Table 1-1 Output Fields of the show ip redirects Command

Field	Description
Default Gateway	Indicates the IP address of the default gateway.

Notifications

N/A

Platform Description

This command is supported after the **no ip routing** command is used on devices.

1.18 show ipv6 redirects

Function

Run the **show ipv6 redirects** command to display the IPv6 default gateway.

Syntax

show ipv6 redirects

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the gateway configuration of a device. This command can be used after the **no ipv6 unicast-routing** command is used on devices.

Examples

The following example displays the IPv6 default gateway.

```
Hostname> enable
Hostname# show ipv6 redirects
Default Gateway: 10::1
```

Table 1-2 Output Fields of the show ipv6 redirects Command

Field	Description
Default Gateway	Indicates the IPv6 address of the default gateway.

Notifications

N/A

Platform Description

This command is supported after the **no ipv6 unicast-routing** command is used on devices.

1 RIP Commands

Command	Function
address-family	Enter address family submode to configure the Routing Information Protocol (RIP).
auto-summary	Enable the automatic summarization function of RIP routes.
bfd all-interfaces	Configure link detection through bidirectional forwarding detection (BFD) for all the interfaces of RIP.
default-information originate	Generate a default route in the RIP process.
default-metric	Configure the default metric for RIP.
distance	Configure the management distance of a RIP route.
distribute-list in	Configure and control route update processing to implement route filtering.
distribute-list out	Configure and control route update advertisement to implement route filtering.
enable mib-binding	Bind the management information base (MIB) with a specified RIP instance.
exit-address-family	Exit the address family configuration mode.
fast-reroute	Configure the RIP fast reroute function of a device.
graceful-restart	Configure the graceful restart (GR) function of a device.
ip rip authentication key-chain	Enable RIP authentication and specify the key chain to be used for RIP authentication.
ip rip authentication mode	Configure the mode of RIP authentication.
ip rip authentication text-password	Enable RIP authentication and set the character string of plain text authentication.
ip rip bfd	Configure BFD for link detection on the specified interface.
ip rip default-information	Configure default route advertisement on a RIP interface.

ip rip receive enable	Allow RIP to receive RIP packets on the specified interface.
ip rip receive version	Define the version of RIP packets to be received by RIP on the specified interface.
ip rip send enable	Allow RIP to send RIP packets on the specified interface.
ip rip send supernet-routes	Allow RIP to send supernetting routes on the specified interface.
ip rip send version	Define the version of RIP packets to be sent by RIP on the specified interface.
ip rip split-horizon	Enable the split horizon function of RIP.
ip rip subvlan	Enable the RIP function on a super VLAN.
ip rip summary-address	Configure the RIP route summarization on an interface.
ip rip triggered	Enable the RIP triggered updates function of demand circuits, and configure the retransmission time and retransmission times of the RIP triggered updates.
ip rip v2-broadcast	Allow RIPv2 packets to be broadcast on the specified interface.
neighbor	Configure the IP address of a RIP neighbor.
network	Configure the list of networks to be advertised by the RIP routing process.
offset-list	Increase the metric of a received or sent RIP route.
output-delay	Set the sending delay between RIP update packets.
passive-interface	Prohibit an interface from sending RIP update packets.
redistribute	Redistribute the external routing information.
router rip	Create a RIP routing process and enter routing process configuration mode.
show ip rip	Display the basic information of a RIP routing protocol process.
show ip rip database	Display the route summary in a RIP route database.

show ip rip external	Display the information about external routes redistributed by RIP.
show ip rip interface	Display the information about a RIP interface.
show ip rip peer	Display the information about a RIP neighbor.
timers basic	Adjust the clock of RIP.
validate-update-source	Validate the source address of a received RIP route update packet.
version	Configure the RIP version No. of the entire device.

1.1 address-family

Function

Run the **address-family** command to enter address family submode to configure the Routing Information Protocol (RIP).

Run the **no** form of this command to delete the address family configured with a routing protocol.

The address family of RIP is disabled by default.

Syntax

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

Parameter Description

vrf *vrf-name*: Specifies the name of the VRF associated with address family configuration submode.

Command Modes

Routing configuration mode

Default Level

14

Usage Guidelines

You can run the **address-family** command to enter address family configuration submode. When the VRF associated with the address family configuration submode is specified for the first time, a RIP instance corresponding to the VRF will be created. In this submode, you can configure the RIP routing information for the related VRF.

To exit address family configuration submode and return to routing process configuration mode, you can run the **exit-address-family** or **exit** command.

Examples

The following example enters the VPN1 address family submode to configure the RIP routing protocol, and create a corresponding RIP instance for the VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf vpn1
Hostname(config-vrf)# exit
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip vrf forwarding vpn1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Hostname(config)# router rip
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# network 192.168.1.0
Hostname(config-router-af)# exit-address-family
```

Notifications

When the VRF associated with the address family does not exist, the following notification will be displayed:

```
% VRF vpn1 doesn't exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

router rip

1.2 auto-summary

Function

Run the **auto-summary** command to enable the automatic summarization function of RIP routes.

Run the **no** form of this command to disable the automatic summarization function of RIP routes.

The automatic summarization function of RIP routes is enabled by default.

Syntax

auto-summary

no auto-summary

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Automatic summarization of RIP routes means that multiple subnet routes are automatically summarized into a classful network route when they cross the boundary of a classful network. For RIPv1 and RIPv2, routes are automatically summarized by default.

If a summarized route exists, subroutes included in the summarized route cannot be seen in the routing table, which reduces the size of the routing table.

Advertising a summarized route is more efficient than advertising individual routes because:

- A summarized route is processed preferentially when RIP looks through the database.
- All subroutes are ignored when RIP looks through the database, which reduces the processing time required.

To learn specific subnet routes, you can disable automatic route summarization. Automatic route summarization can only be disabled using RIPv2. The range of supernetting routes is larger than that of the classful network. Therefore, this command is invalid for supernetting routes.

Examples

The following example disables automatic route summarization of RIPv2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# version 2
Hostname(config-router)# no auto-summary
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to configure link detection through bidirectional forwarding detection (BFD) for all the interfaces of RIP.

Run the **no** form of this command to restore the default configuration.

The BFD function is disabled by default.

Syntax

bfd all-interfaces

no bfd all-interfaces

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

After BFD is enabled on RIP, a BFD session will be set up for the RIP routing information source (that is, the source address of RIP route update packets). Once the BFD neighbor fails, the corresponding RIP route information directly enters the invalid state and is not forwarded.

You can also run the **ip rip bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the **bfd all-interfaces** command used in routing process configuration mode.

Examples

The following example configures all interfaces running RIP to conduct BFD link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# bfd all-interfaces
```

Notifications

When your peer device also needs to be configured with BFD to prevent route learning from being affected, the following notification will be displayed:

```
% Warning: The BFD for RIP peer shall be enabled, or it would affect the route learning.
```

Common Errors

BFD is not enabled on the interconnected devices at the same time.

Platform Description

N/A

Related Commands

- **show ip rip**

1.4 default-information originate

Function

Run the **default-information originate** command to generate a default route in the RIP process.

Run the **no** form of this command to cancel the generated default route.

There is no default route in the RIP process by default.

Syntax

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *route-map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *route-map-name*]

Parameter Description

always: Enables RIP to generate a default route no matter whether the local router has a default route.

metric *metric-value*: Specifies the initial metric of the default route. The value range is from 1 to 15, and the default value is **1**.

route-map *route-map-name*: Specifies the name of the associated route map. No route map is associated by default.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a default route exists in the routing table of a device, RIP does not advertise the default route to external entities by default. You need to run the configuration command **default-information originate** to advertise the default route to neighbors.

If the RIP process can generate a default route using this command, RIP does not learn the default route advertised by the neighbor.

You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

The parameters are used as follows:

- If the **always** parameter is configured, the RIP routing process advertises a default route to neighbors no matter whether the default route exists, but this default route is not displayed in the local routing table. To check whether the default route is generated, run the **show ip rip database** command to check the RIP routing information database.
- To further control the behavior of advertising the RIP default route, use the **route-map** parameter. For example, run the **set metric** rule to set the metric of the default route.
- You can use the **metric** parameter to set the metric of the advertised default value, but the priority of this configuration is lower than that of the **set metric** rule of the route map. If the **metric** parameter is not configured, the default route uses the default metric configured for RIP.

Examples

The following example generates a default route in the RIP process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config-router)# default-information originate always
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip database**

1.5 default-metric

Function

Run the **default-metric** command to configure the default metric for RIP.

Run the **no** form of this command to restore the default configuration.

By default, the metric of a redistributed route is 1.

Syntax

default-metric *metric-value*

no default-metric

Parameter Description

metric-value: Default metric value. The value range is from 1 to 16. If the value of *metric-value* is equal to or greater than 16, the device determines that this route is unreachable.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command must be used together with the **redistribute** command. When a route is redistributed from another routing protocol process to the RIP route process, the route metric cannot be converted because the metric calculating mechanism is different for each routing protocol. Therefore, in the process of transformation, you need to define the metric of redistributed route in the RIP routing domain. If the metric is not specified during redistribution of a routing protocol process, RIP uses the metric defined by the **default-metric** command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric. If this command is not configured, the value of metric is 1 by default.

Examples

The following example uses the RIP to redistribute the route learned by the Open Shortest Path First (OSPF) routing protocol, and sets the initial RIP metric to **3**.

```
Hostname(config)# router rip
Hostname(config-router)# default-metric 3
Hostname(config-router)# redistribute ospf 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip database**
- **redistribute**

1.6 distance

Function

Run the **distance** command to configure the management distance of a RIP route.

Run the **no** form of this command to restore the default configuration.

The management distance is **120** by default.

Syntax

distance *distance* [*ipv4-address wildcard*]

no distance [*distance ipv4-address wildcard*]

Parameter Description

distance: Management distance of a RIP route. The value range is an integer from 1 to 255.

ipv4-address: Prefix of the source IP address of the route.

wildcard: IP address comparison bit. Value 0 indicates accurate matching, and 1 indicates that no comparison is performed.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the management distance of a RIP route.

You can run this command to create multiple management distances with source address prefixes. When the source address of a RIP route is within the range of these prefixes, the corresponding management distance will be used; otherwise, the management distance set by RIP will be used for the route.

Examples

The following example configures the management distance of RIP route as 160, and specifies the management distance of the route learned from 192.168.12.1 as **123**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# distance 160
Hostname(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Notifications

When the configured mask is incorrect, the following notification will be displayed:

```
% Invalid mask value
```

Common Errors

The configured mask is incorrect.

Platform Description

N/A

Related Commands

- **show ip rip**

1.7 distribute-list in

Function

Run the **distribute-list in** command to configure and control route update processing to implement route filtering.

Run the **no** form of this command to delete the configured inbound distribution list.

There is no inbound distribution list by default.

Syntax

distribute-list { [*acl-number* | *acl-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

no distribute-list { [*acl-number* | *acl-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

Parameter Description

acl-number: ACL No. Only routes permitted by the access list can be received. The following value ranges are supported.

The value range of IP standard ACL is 1 to 99 or 1300 to 1999; the value range of IP extended ACL is 100 to 199 or 2000 to 2699.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters. Only routes permitted by the access list can be received.

prefix *prefix-list-name*: Uses the prefix list to filter routes.

gateway *prefix-list-name*: Uses the prefix list to filter the route sources.

interface-type interface-number: Specified interface only on which the distribution list is used.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.

Examples

The following example configures the RIP routing process to control route update processing over the GigabitEthernet 0/1 interface and allows receiving only routes of the 172.16.0.0/16 address segment of ACL 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# network 200.168.23.0
Hostname(config-router)# distribute-list 10 in GigabitEthernet 0/1
Hostname(config-router)# no auto-summary
Hostname(config)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP Routing Basic)

1.8 distribute-list out

Function

Run the **distribute-list out** command to configure and control route update advertisement to implement route filtering.

Run the **no** form of this command to delete route update advertisement control to implement route filtering.

There is no outbound distribution list by default.

Syntax

distribute-list { [*acl-name* | *acl-number*] | **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *acl-name* | *acl-number* | **prefix** *prefix-list-name* } **out** [*interface-type interface-numbe* | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

acl-number: ACL No. Only routes permitted by the access list can be sent. The following value ranges are supported.

The value range of IP standard ACL is 1 to 99 or 1300 to 1999; the value range of IP extended ACL is 100 to 199 or 2000 to 2699.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters. Only routes permitted by the access list can be sent.

prefix *prefix-list-name*: Uses the prefix list to filter routes.

interface-type interface-number: Specified interface only to which the route update advertisement control is applicable.

bgp: Applies route update advertisement control only to the routes introduced from Border Gateway Protocol (BGP).

connected: Applies route update advertisement control only to the routes introduced through direct connection.

isis [*area-tag*]: Applies route update advertisement control only to the routes introduced from Intermediate System to Intermediate System (IS-IS). Here, *area-tag* specifies an IS-IS instance.

ospf *process-id*: Applies route update advertisement control only to the routes introduced from OSPF. Here, *process-id* specifies an OSPF instance.

rip: Applies route update advertisement control only to RIP routes.

static: Applies route update advertisement control only to static routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

- If this command is configured without any optional parameters, route update advertisement control takes effect on all the interfaces.
- If any interface option is configured, route update advertisement control takes effect on the specified interface only.
- If other routing process parameters are configured, route update advertisement control takes effect on the specified routing processes only.

Examples

The following example configures the RIP routing process to control route update advertisement processing and allows externally advertising only routes of the 192.168.12.0/24 address segment of ACL 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# network 200.4.4.0
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# distribute-list 10 out
Hostname(config-router)# version 2
Hostname(config)# access-list 10 permit 192.168.12.0 0.0.0.255
```

Notifications

When gateway filtering cannot be used for **out** configuration by default, the following notification will be displayed:

```
% Gateway not allowed with OUT in distribute-list cmd
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route rip** (IP Routing Basic)

1.9 enable mib-binding

Function

Run the **enable mib-binding** command to bind the management information base (MIB) with a specified RIP instance.

Run the **no** form of this command to restore the default binding.

By default, the MIB is bound with the RIP instance of the default VRF.

Syntax

enable mib-binding

no enable mib-binding

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The RIP MIB does not have RIP instance information. Therefore, you must perform operations only on one instance through SNMP. By default, the RIP MIB is bound with the RIP instance of the default VRF, and all user operations take effect on this instance.

If you wish to perform operations on a specified RIP instance through SNMP, run this command to bind the MIB with the instance.

Examples

The following example configures to bind MIB to the specified RIP instance, and operate the RIP instance with VRF as VPN 1 through SNMP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 exit-address-family

Function

Run the **exit-address-family** command to exit the address family configuration mode.

This command has no default behavior or value.

Syntax

exit-address-family

Parameter Description

N/A

Command Modes

Address family configuration mode

Default Level

14

Usage Guidelines

This command is used in address family configuration mode to exit this configuration mode. This command can be abbreviated as **exit**.

Examples

The following example configures to enter and exit the address family configuration submode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# exit-address-family
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 fast-reroute

Function

Run the **fast-reroute** command to configure the RIP fast reroute function of a device.

Run the **no** form of this command to restore the default configuration.

The fast reroute function is disabled by default.

Syntax

fast-reroute route-map *route-map-name*

no fast-reroute

Parameter Description

route-map-name: Route map through which the backup path is specified.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the RIP fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface switches Up/Down, to shorten the forwarding interruption time during RIP fast reroute, you can configure **carrier-delay 0** in interface configuration mode to achieve the fastest switchover speed. If the route map is configured, a backup path can be specified for a matched route through the route map.

Currently, the RIP fast reroute function is subject to the following constraints:

- Only one backup next hop can be generated for one route.
- No backup next hop can be generated for equal-cost multi-path routing (ECMP).

Examples

The following example configures the RIP FRR function of a device and associates it with route map fast-reroute. It configures route map fast-reroute, matches the interface Gigabit Ethernet 0/2, and sets the FRR backup interface to Gigabit Ethernet 0/1 and the backup next hop to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map fast-reroute
Hostname(config-route-map)# match interface gigabitEthernet 0/2
Hostname(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1
backup-nexthop 192.168.1.1
Hostname(config)# router rip
Hostname(config-router)# fast-reroute route-map fast-reroute
```

Notifications

When the name length of the configured route map exceeds the maximum value, the following notification will be displayed:

```
% Route-map name string length can not exceed 32
```

When the configured route map does not exist, the following notification will be displayed:

```
% route-map name not exist
```

Common Errors

The name length of the configured route map is too long.

The configured route map does not exist.

Platform Description

N/A

Related Commands

N/A

1.12 graceful-restart

Function

Run the **graceful-restart** command to configure the graceful restart (GR) function of a device.

Run the **no** form of this command to restore the default configuration.

The GR function is enabled by default.

Syntax

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

graceful-restart: Enables the GR function.

grace-period *grace-period*: Specifies the GR period, in seconds. The value range is 1 to 1800. The default value is twice the update time or 60s, whichever is the smaller.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The GR function is configured based on the RIP process. You can configure different parameters for different RIP processes based on the actual conditions.

The GR period is the maximum time from restart of the RIP process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIP route is restored so as to restore the RIP state before the restart. After the restart period expires, RIP exits the GR state and performs common RIP operations.

The **graceful-restart grace-period** command allows you to explicitly modify the GR period. Note that GR must be completed after the update timer of the RIP route expires and before the invalid timer of the RIP route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are not advised to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalidity timer based on the configuration of the **timers basic** command.

During the RIP GR process, ensure that the network environment is stable.

Examples

The following example configures the RIP GR function of a device, and sets the GR period parameter to 80s:

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# graceful-restart grace-period 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip**

1.13 ip rip authentication key-chain

Function

Run the **ip rip authentication key-chain** command to enable RIP authentication and specify the key chain to be used for RIP authentication.

Run the **no** form of this command to delete the specified key chain.

No key chain is set by default.

Syntax

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter Description

name-of-keychain: Name of the key chain used for RIP authentication.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a key chain is already specified in the interface configuration, you need to run the **key chain** command in global configuration mode to define the key chain; otherwise, authentication of RIP packets may fail.

If this command and the **ip rip authentication mode md5** command are configured, message digest 5 (MD5) mode authentication is adopted. If the **ip rip authentication mode** command is not configured, authentication is performed according to the authentication mode specified by the configured **key chain**. MD5 authentication and SM3 authentication are supported at present. Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Examples

The following example enables RIP authentication on the GigabitEthernet 0/1 interface and specifies the key chain used for RIP authentication as **ripchainf**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain ripchain
```

The following example configures the key chain as **ripchain** and the key 1 string as **Hello**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# key chain ripchain
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string Hello
```

Notifications

N/A

Common Errors

When MD5 authentication is configured, **key-chain** is not configured first.

Platform Description

N/A

Related Commands

- **ip rip authentication mode**
- **show ip rip interface**

1.14 ip rip authentication mode

Function

Run the **ip rip authentication mode** command to configure the mode of RIP authentication.

Run the **no** form of this command to restore the default RIP authentication mode.

Plain text authentication mode is used by default.

Syntax

ip rip authentication mode { **text** | **md5** }

no ip rip authentication mode

Parameter Description

text: Indicates that the RIP authentication mode is plain text authentication.

md5: Indicates that the RIP authentication mode is MD5 authentication.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

The RIP authentication modes configured on all devices that need to directly exchange RIP routing information must be the same; otherwise, exchange of RIP packets may fail.

Use plain text or MD5 authentication as instructed below:

- If plain text authentication is used, but the key chain for plain text authentication is not configured or associated, authentication is not performed.
- If MD5 authentication is used, but the key chain is not configured or associated, authentication is not performed either.

Examples

The following example configures the RIP authentication mode of GigabitEthernet 0/1 interface as **MD5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**
- **ip rip authentication key-chain**
- **ip rip authentication text-password**

1.15 ip rip authentication text-password

Function

Run the **ip rip authentication text-password** command to enable RIP authentication and set the character string of plain text authentication.

Run the **no** form of this command to delete the character string of plain text authentication.

No character string of plain text authentication is set by default.

Syntax

ip rip authentication text-password [**0** | **7**] *password-string*

no ip rip authentication text-password

Parameter Description

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

password-string: Character string used for plain text authentication. The length range is 1 to 16 bytes.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command takes effect only in plain text authentication mode. If RIP plain text authentication should be enabled, run this command to configure the key chain for plain text authentication. Alternatively, you can obtain the key chain for plain text authentication by associating the key chain. The key chain obtained using the second method takes precedence over that obtained using the first method.

Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Examples

The following example configures the RIP authentication mode of GigabitEthernet 0/1 interface as plain text authentication and sets the character string of plain text authentication to **hello**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip authentication text-password hello
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip rip authentication mode**
- **show ip rip interface**

1.16 ip rip bfd

Function

Run the **ip rip bfd** command to configure BFD for link detection on the specified interface.

Run the **no** form of this command to delete the BFD configured on the interface.

By default, BFD link detection on an interface is disabled by default.

Syntax

ip rip bfd [**disable**]

no ip rip bfd

Parameter Description

disable: Disables BFD for link detection on a specified interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The BFD configured on an interface takes precedence over the **bfd all-interfaces** command used in process configuration mode.

In light of the actual environment, you can run the **ip rip bfd** command to configure BFD for link detection on the specified interface, or run the **bfd all-interfaces** command to configure BFD for link detection on all the interfaces. You can run the **ip rip bfd disable** command to disable BFD for link detection on the specified interface.

Examples

The following example enables BFD for link detection on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip bfd
```

Notifications

When your peer device also needs to be configured with BFD to prevent route learning from being affected, the following notification will be displayed:

```
% Warning: The BFD for RIP peer shall be enabled, or it would affect the route learning.
```

Common Errors

BFD is not enabled on the interconnected devices at the same time.

Platform Description

N/A

Related Commands

- **show ip rip**

1.17 ip rip default-information

Function

Run the **ip rip default-information** command to configure default route advertisement on a RIP interface.

Run the **no** form of this command to cancel default route advertisement on the specified interface.

By default, default route advertisement is disabled on an interface.

Syntax

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ip rip default-information

Parameter Description

only: Indicates that only the default route is advertised.

originate: Indicates that the default route and other routes are advertised.

metric *metric-value*: Specifies the metric of the default route. The value range is from 1 to 15, and the default value is **1**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured on an interface, a default route is generated and advertised through this interface. If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process, only the default route configured for the interface is advertised.

So far as the **ip rip default-information** command is configured for an interface, RIP does not learn the default route advertised by the neighbor.

Examples

The following example configures default route advertisement on RIP ethernet0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip default-information only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**

1.18 ip rip receive enable

Function

Run the **ip rip receive enable** command to allow RIP to receive RIP packets on the specified interface.

Run the **no** form of this command to forbid RIP from receiving RIP packets on the specified interface.

By default, the RIP packet receiving function is enabled on an interface.

Syntax

ip rip receive enable

no ip rip receive enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To prohibit receiving RIP packets on a specified interface, you can run the **no** form of this command in interface configuration mode. This command takes effect only on the current interface. You can run the **default** form of this command to restore the default setting, that is, allowing the interface to receive RIP packets.

Examples

The following example prohibits receiving of RIP packets on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip rip receive enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**

1.19 ip rip receive version

Function

Run the **ip rip receive version** command to define the version of RIP packets to be received by RIP on the specified interface.

Run the **no** form of this command to restore the default configuration.

By default, the default behavior depends on the configuration of the **version** command.

Syntax

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter Description

version 1: Indicates that only RIPv1 packets are received.

version 2: Indicates that only RIPv2 packets are received.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of receiving RIP packets on the current interface, and the interface is allowed to receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets depends on the configuration of the **version** command.

Examples

The following example allows receiving RIPv1 and RIPv2 packets on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip receive version 1 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**
- **show ip rip**

1.20 ip rip send enable

Function

Run the **ip rip send enable** command to allow RIP to send RIP packets on the specified interface.

Run the **no** form of this command to forbid RIP from sending RIP packets on the specified interface.

By default, the RIP packet sending function is enabled on an interface.

Syntax

ip rip send enable

no ip rip send enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To prohibit sending of RIP packets on a specified interface, you can run the **no** form of this command in interface configuration mode. This command takes effect only on the current interface. You can run the **default** form of this command to restore the default setting, that is, allowing the interface to send RIP packets.

Examples

The following example prohibits RIP from sending RIP packets on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip rip send enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**

1.21 ip rip send supernet-routes

Function

Run the **ip rip send supernet-routes** command to allow RIP to send supernetting routes on the specified interface.

Run the **no** form of this command to forbid RIP from sending supernetting routes on the specified interface.

By default, the supernetting route sending function is enabled on an interface.

Syntax

ip rip send supernet-routes

no ip rip send supernet-routes

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a supernetting route is detected when a RIPv1-enabled router monitors RIPv2 route response packets, the router will learn an incorrect route because RIPv1 ignores the subnet mask in the routing information of the packet. In this case, the **no** form of the command must be used to prohibit advertisement of supernetting routes on the related interface. This command takes effect only on the current interface.

The command is effective only when RIPv2 packets are sent on the interface, and is used to control the sending of supernetting routes.

Examples

The following example prohibits RIP from sending RIP supernetting routes on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip rip send version

Function

Run the **ip rip send version** command to define the version of RIP packets to be sent by RIP on the specified interface.

Run the **no** form of this command to restore the default configuration.

By default, the default behavior depends on the configuration of the **version** command.

Syntax

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter Description

1: Indicates that only RIPv1 packets are sent.

2: Indicates that only RIPv2 packets are sent.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the current interface, and the interface can receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of sending RIP packets depends on the configuration of the version command.

Examples

The following example configures the specific version of RIP packets to be sent by RIP on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip send version 1 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**
- **show ip rip**

1.23 ip rip split-horizon

Function

Run the **ip rip split-horizon** command to enable the split horizon function of RIP.

Run the **no** form of this command to disable the split horizon function of RIP.

By default, the split horizon function without poison reverse is enabled.

Syntax

ip rip split-horizon [**poisoned-reverse**]

no ip rip split-horizon [**poisoned-reverse**]

Parameter Description

poisoned-reverse: Enables split horizon with poison reverse.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When multiple devices are connected to an IP broadcast-type network and run the distance vector routing protocols at the same time, you must adopt the split horizon mechanism to avoid the formation of route loop.

For a non-broadcast multi-access network such as frame relay and X.25 network, split horizon may prevent some devices from learning the complete routing information. In this case, you may need to disable split horizon. If an interface is configured with a secondary IP address, the problem of split horizon also needs to be noted.

If the **poisoned-reverse** parameter is configured, the split horizon with poison reverse will be enabled, and the device will still advertise the routing information from the interface that has learned the routing information, but set the metric of the routing information to a value unreachable.

The RIP routing protocol falls into distance vector routing protocols, so the problem of split horizon must be noted in the actual application. If you cannot determine whether split horizon has been enabled on an interface, you can run the **show ip rip** command to make judgment. In addition, the neighbors defined using the **neighbor** command will not be affected by RIP split horizon.

Examples

The following example disables RIP split horizon on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip rip split-horizon
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**
- **show ip rip**

1.24 ip rip subvlan

Function

Run the **ip rip subvlan** command to enable the RIP function on a super VLAN.

Run the **no** form of this command to restore the default configuration.

By default, RIP is disabled on a super VLAN.

Syntax

ip rip subvlan [**all** | *vid*]

no ip rip subvlan

Parameter Description

all: Allows sending packets to all sub VLANs.

vid: Sub VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are replicated once and sent to all of its sub VLANs. In this case, when RIP multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIP multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the RIP function does not need to be enabled on a super VLAN. However, in some scenarios, the RIP function is required on the super VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. Usually, packets need to be sent to only one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the RIP function on Super VLAN 300 and allows sending RIP multicast packets to Sub VLAN 2014.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# ip rip subvlan 1024
```

Notifications

N/A

Common Errors

The function is configured on a non-super VLAN.

The specified sub VLAN on the super VLAN cannot interwork with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.25 ip rip summary-address

Function

Run the **ip rip summary-address** command to configure the RIP route summarization on an interface.

Run the **no** form of this command to disable RIP route summarization for the specified address or subnet.

By default, RIP route summarization is not configured on an interface.

Syntax

ip rip summary-address *ipv4-address mask*

no ip rip summary-address *ipv4-address mask*

Parameter Description

ipv4-address: IP address to be summarized.

Mask: Subnet mask of the IP address to be summarized.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to manually summarize an address or a subnet under a specified interface. The summary range configured by this command cannot cover supernetting routes, that is, the configured subnet mask length cannot be smaller than the natural mask length of the network.

Examples

The following example disables automatic route summarization of RIPv2. Summarization is configured on the GigabitEthernet 0/1 Interface, and GigabitEthernet 0/1 will advertise the route 172.16.0.0/16 after summarization.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# network 172.16.0.0
Hostname(config-router)# version 2
Hostname(config-router)# no auto-summary
Hostname(config-router)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
```

Hostname(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0Notifications

When the entered mask is wrong and you need to use the correct mask, the following notification will be displayed:

```
RIP: Invalid mask input
```

When the address to be summarized is wrong, for example, 0 address, the following notification will be displayed:

```
% Invalid summary-address value.
```

When the mask to be summarized is not longer than the mask of the main network, the following notification will be displayed:

```
% Summary mask must be greater or equal to major net.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ip rip triggered

Function

Run the **ip rip triggered** command to enable the RIP triggered updates function of demand circuits, and configure the retransmission time and retransmission times of the RIP triggered updates.

Run the **no** form of this command to disable the RIP triggered updates function of demand circuits, and cancel the configured retransmission time and retransmission times of the RIP triggered updates.

The RIP triggered updates function is disabled by default.

Syntax

ip rip triggered [**retransmit-timer** *timer* | **retransmit-count** *count*]

no ip rip triggered [**retransmit-timer** *timer* | **retransmit-count** *count*]

Parameter Description

retransmit-timer *timer*: Configures the interval at which the Update Request or Update Response packet is retransmitted, in seconds. The value range is 1 to 3600, and the default value is **5**.

retransmit-count *count*: Configures the maximum retransmission times of the Update Request or Update Response packet. The default value is **36** times. The value range is from 1 to 3600, and the default value is **36**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The RIP triggered updates function is the extension of RIP on the wide area network (WAN), and mainly used for demand circuits.

After the RIP triggered updates function is enabled, RIP does not periodically send the route update packets. RIP sends the route update packets to the WAN interface only in one of the following cases:

- A route request packet is received.
- The RIP routing information changes.
- The interface state changes.
- The router is started.

Since the RIP periodical update function is disabled, the acknowledgment and retransmission mechanisms must be used to ensure that the update packets are successfully sent or received on the WAN. You can use the **retransmit-timer** and **retransmit-count** parameters to specify the retransmission interval and maximum retransmission times of the request and update packets.

The triggered updates function can be enabled in either of the following cases:

- The interface has only one neighbor.
- The interface has multiple neighbors but the device interacts with these neighbors in unicast mode.

You are advised to enable this function on the PPP, frame relay, or X.25 link layer protocol.

Precautions for using the triggered updates function:

- It is recommended that split horizon with poison reverse be enabled on the interface configured with the triggered updates function; otherwise, invalid routing information may exist.
- Ensure that this function is enabled on all the routers on the same link; otherwise, this function fails and the routing information cannot be exchanged properly.

- This function cannot be enabled together with the function of correlating RIP with BFD.
- To enable the triggered updates function, make sure that the RIP configurations at both ends of the link are consistent, such as RIP authentication and the RIP protocol version supported by the interface.
- If the triggered updates function is enabled on an interface, source address verification is performed on the packets of this interface no matter whether the source address verification function is enabled using the **validate-update-source** command.

Examples

The following example enables the RIP triggered updates function of demand circuits, and configures the retransmission time as 10s and retransmission times as 18

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip triggered
Hostname(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10
Hostname(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18
```

Notifications

When enabling the RIP triggered updates function may affect route learning, the following notification will be displayed:

```
% Warning: The configurations for Triggered RIP peer shall be same, or it would affect
the route learning.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 ip rip v2-broadcast

Function

Run the **ip rip v2-broadcast** command to allow RIPv2 packets to be broadcast on the specified interface.

Run the **no** form of this command to restore the default configuration.

By default, RIPv2 packets are multicast on an interface.

Syntax

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the link or neighbor does not support multicasting, you can configure to broadcast RIPv2 packets.

Examples

The following example allows broadcasting RIPv2 packets on the interface, instead of multicasting.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip rip v2-broadcast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**

1.28 neighbor

Function

Run the **neighbor** command to configure the IP address of a RIP neighbor.

Run the **no** form of this command to delete a neighbor.

No RIP neighbor is configured by default.

Syntax

neighbor *ipv4-address*

no neighbor *ipv4-address*

Parameter Description

ipv4-address: IP address of the neighbor. It should be the address of the network directly connected to the local device.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise the routing information, whereas RIPv2 uses the multicast address (224.0.0.9) to advertise the routing information. If you do not want all devices on the broadcast network or non-broadcast multiple access (NBMA) network to receive routing information, configure the related interface as the passive interface using the **passive-interface** command, and specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send a request packet even after the device is restarted.

Examples

The following example configures the IP address of a RIP neighbor as 192.168.1.2, and the interface of RIP as passive interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# passive-interface default
Hostname(config-router)# neighbor 192.168.1.2
```

Notifications

When the same configuration already exists, the following notification will be displayed:

```
% Static neighbor configuration exists
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **passive-interface**

1.29 network

Function

Run the **network** command to configure the list of networks to be advertised by the RIP routing process.

Run the **no** form of this command to delete the configured network.

No local network is advertised by default.

Syntax

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description

network-number: No. of the direct network. This is a natural network No., and all the interfaces with an IP address belonging to the natural network can send and receive RIP packets.

wildcard: IP address comparison bit. Value 0 indicates accurate matching, and 1 indicates that no comparison is performed.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can configure the *network-number* and *wildcard* parameters at the same time to enable the interface addresses in the address range to participate in RIP running.

If *wildcard* is not configured, the classful address range is used by default, that is, the device will allow the interfaces whose addresses fall into the classful address range to participate in RIP running.

Only when the interface address is in the network list defined by RIP, can the interface send and receive RIP route update packets.

Examples

The following example configures the networks to be notified by the RIP routing process as 192.168.12.0/24 and 172.16.0.0/24.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# network 172.16.0.0 0.0.0.255
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip interface**

1.30 offset-list

Function

Run the **offset-list** command to increase the metric of a received or sent RIP route.

Run the **no** form of this command to delete the specified offset list.

No offset list is configured by default.

Syntax

offset-list { *acl-number* | *acl-name* } { **in** | **out** } *offset* [*interface-type interface-number*]

no offset-list { *acl-number* | *acl-name* } { **in** | **out** } *offset* [*interface-type interface-number*]

Parameter Description

acl-number: ACL No. The following value ranges are supported.

The value range of IP standard ACL is 1 to 99 or 1300 to 1999; the value range of IP extended ACL is 100 to 199 or 2000 to 2699.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

in: Uses the ACL to modify the metric of a received route.

out: Uses the ACL to modify the metric of a sent route.

offset: Offset of the modified metric. The value range is from 0 to 16.

interface-type: Specified interface where the ACL is used.

Interface-number:-number: Interface number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can use this function to increase the metric of a received or sent RIP route. If a RIP route satisfies both the offset-list of the specified interface and the global offset-list without a specified interface, this RIP route will be increased by the metric of the offset-list of the specified interface.

Examples

The following example increases the metric of the sent RIP route matched with ACL 7 by 7.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# offset-list 7 out 7
```

The following example increases the metric of the RIP route that is matched with ACL 7 and received on GigabitEthernet0/1 by 7.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# offset-list 8 in 7 GigabitEthernet 0/1
```

Notifications

When an interface does not exist or is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip database**

1.31 output-delay

Function

Run the **output-delay** command to set the sending delay between RIP update packets.

Run the **no** form of this command to cancel the sending delay between RIP update packets.

The sending delay between RIP update packets is 0 by default.

Syntax

output-delay *delay*

no output-delay

Parameter Description

delay: Sending delay between packets, in milliseconds. The value range is from 8 to 50.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Normally, a RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible.

When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may not be able to process all update packets in time, causing loss of routing information. In this case, you need to run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Examples

The following example changes the sending delay between RIP update packets to 30 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# output-delay 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 passive-interface

Function

Run the **passive-interface** command to prohibit an interface from sending RIP update packets.

Run the **no** form of this command to enable an interface to send RIP update packets.

By default, a RIP-enabled interface is allowed to send and receive RIP update packets normally.

Syntax

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

default: Indicates that all interfaces will be configured as passive interfaces.

interface-type interface-num: Interface type and interface number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

A passive interface suppresses RIP update packets. A passive interface defines the boundary of RIP routing domain to avoid unwanted flooding of RIP packets. If the interface connection device does not run the RIP routing protocol (such as a PC, and Layer-3 device running other routing protocols), you are advised to configure this interface as a passive interface. You can run the **passive-interface default** command to configure all interfaces as passive interfaces, and run the **no passive-interface** *interface-type interface-num* command to configure the specified interface as a non-passive interface.

The passive interface no longer sends RIP route update packets, but can still receive RIP route update packets. In this case, you can run the **neighbor** command on the interface to send route update packets to the specified neighbor.

To fully control whether an interface can send and receive route update packets, you can run the **ip rip send enable** and **ip rip receive enable** commands.

Examples

The following example configures all interfaces as the passive mode, and then sets GigabitEthernet 0/1 to non-passive mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface GigabitEthernet 0/1
```

Notifications

When an interface does not exist or is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip**
- **show ip rip interface**

1.33 redistribute

Function

Run the **redistribute** command to redistribute the external routing information.

Run the **no** form of this command to cancel redistribution of external routes.

The external routing information is not redistributed to RIP by default.

If OSPF redistribution is configured, the routes of all sub-types of the instance will be redistributed.

If IS-IS redistribution is configured, the routes of Level-2 sub-type of the instance will be redistributed.

In other cases, all routes of this type are redistributed.

Syntax

redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **static** } [**metric** | **route-map**] *

Parameter Description

bgp: Redistributes from BGP.

connected: Redistributes from direct routes.

isis *area-tag*: Redistributes from IS-IS. *area-tag* indicates the IS-IS process ID.

l**evel-1** | **level-2** | **level-1-2**: Redistributes IS-IS routes at the specified level.

static: Redistributes from static routes.**match**: Redistributes specific OSPF routes that match the filtering conditions.

external [**1** | **2**]: Redistributes E1, E2, or all external routes.

internal: Redistributes internal routes and inter-area routes.

nssa-external [**1** | **2**]: Redistributes N1, N2, or all external routes of all NSSAs.

metric *metric-value*: Sets the metric of the redistributed route. The value range is from 1 to 16, and the default value is **1**.

route-map *route-map-name*: Associates route map, which is used to set the redistribution filtering rules.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used to redistribute external routing information to RIP.

During route redistribution, different routing protocols use different metric measurement methods. For example, RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, however, it is necessary to configure a symbolic metric; otherwise, route redistribution fails.

If you configure redistribution of IS-IS routes without specifying the level parameter, only level-2 routes can be redistributed by default. If you specify the **level** parameter during initial configuration of redistribution, routes of the specified level can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.

If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be redistributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.

The configuration rules for the **no** form of the **redistribute** command are as follows:

- If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
- If no parameter is specified in the **no** form of this command, the entire command will be deleted.

For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the

configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed.

To delete the entire command, run the **no redistribute isis 112** command.

Note

The route redistribution command cannot introduce default routes of other protocols to the RIP routing domain. To introduce default routes to the RIP routing domain, run the **default-information originate** command.

Examples

The following example configures static route redistribution to the RIP routing domain.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# redistribute static
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip database**

1.34 router rip

Function

Run the **router rip** command to create a RIP routing process and enter routing process configuration mode.

Run the **no** form of this command to delete a RIP routing process.

The RIP routing process is disabled by default.

Syntax

router rip

no router rip

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To create a RIP routing process, you need to define a network No. If a dynamic routing protocol runs on an asynchronous line, **async default routing** needs to be configured on the asynchronous interface.

Examples

The following example creates a RIP routing process and enters routing process configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip rip**

1.35 show ip rip

Function

Run the **show ip rip** command to display the basic information of a RIP routing protocol process.

Syntax

show ip rip [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Specifies the RIP information of the specified VRF.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command can be used to quickly display the three timers, route distribution, route redistribution status, RIP version of interface, RIP interface, network scope, metric, management distance, and other information of a RIP routing protocol process. If VRF is specified, the VRF name and VRF-ID will also be displayed.

Examples

The following example displays the basic information of a RIP routing protocol process.

```
Hostname> enable
Hostname# show ip rip
Routing Protocol is "rip"
Sending updates every 10 seconds
Invalid after 20 seconds, flushed after 10 seconds
Outgoing update filter list for all interface is: not set
Incoming update filter list for all interface is: not set
Default redistribution metric is 2
Redistributing: connected
Default version control: send version 2, receive version 2
Interface            Send  Recv
GigabitEthernet 0/1      2    2
GigabitEthernet 0/2      2    2
Routing for Networks:
192.168.26.0 255.255.255.0
192.168.64.0 255.255.255.0
Distance: (default is 50)
Graceful-restart enabled
 Restart grace period 60 secs
 Current Restart remaining time 16 secs
```

The following example displays the basic information of the corresponding RIP instance of VRF 1.

```
Hostname> enable
Hostname# show ip rip vrf 1
VRF 1  VRF-id:1
Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, flushed after 120 seconds
Outgoing update filter list for all interface is: not set
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 1, receive any version
Routing for Networks:
Distance: (default is 120)
Graceful-restart disabled
```

Table 1-1 Output Fields of the show ip rip Command

Field	Description
Sending updates	Indicates the packet update time.
Invalid	Indicates the failure time.
flushed	Indicates the refreshing time.
Outgoing update filter list for all interface	Filters all the output routes.
Incoming update filter list for all interface	Filters all the received routes.
Default redistribution metric	Indicates the default redistribution metric configured.
Redistributing	Indicates the redistributing protocol.
Default version control	Indicates the default RIP protocol version running for the instance.
Routing for Networks:	Indicates the routing network segment externally advertised by RIP.
Distance	Indicates the management distance of an instance.
Graceful-restart	Indicates whether the GR function is enabled.
Restart grace period	Indicates the GR time.
Current Restart remaining time	Indicates the remaining GR time.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.36 show ip rip database

Function

Run the **show ip rip database** command to display the route summary in a RIP route database.

Syntax

show ip rip database [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]

Parameter Description

vrf *vrf-name*: Specifies the VRF whose RIP routing information is displayed.

network-number: Subnet No. of routing information.

network-mask: Subnet mask. If a network number has been set, you must specific a subnet mask.

count: Displays the routing statistics summary in a RIP database.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Only when the related subroutes are summarized, will the summarized address item information be displayed in the RIP route database. When the information of the last subroute of the summarized address item information becomes invalid, the summarized address item information will also be deleted from the database.

Examples

The following example displays the route summary in a RIP route database.

```
Hostname> enable
Hostname# show ip rip database
192.168.1.0/24     auto-summary
192.168.1.0/30     directly connected, Loopback 3
192.168.1.8/30     directly connected, GigabitEthernet 0/1
192.168.121.0/24   auto-summary
192.168.121.0/24   redistributed
[1] via 192.168.2.22, GigabitEthernet 0/2
192.168.122.0/24   auto-summary
192.168.122.0/24
[1] via 192.168.4.22, GigabitEthernet 0/1  00:28   permanent
```

The following example displays the summarized address item information of 192.168.121.0/24 in a RIP route database.

```
Hostname> enable
Hostname# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24   redistributed
[1] via 192.168.2.22, GigabitEthernet 0/1
```

The following example displays the statistics summary of each route type in a RIP route database.

```
Hostname> enable
Hostname# show ip rip database count
             All    Valid   Invalid
database       5      5      0
auto-summary    5      5      0
connected      1      1      0
rip           4      4      0
```

Table 1-2 Output Fields of the show ip rip database Command

Field	Description
auto-summary	Indicates the summarized route.
directly connected	Indicates the direct route.
redistributed	Indicates the redistributed route.
database	Indicates the route database of RIP.
All	Indicates the count of all routes.
Valid	Indicates the count of valid routes.
Invalid	Indicates the count of invalid routes.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.37 show ip rip external

Function

Run the **show ip rip external** command to display the information about external routes redistributed by RIP.

Syntax

show ip rip external [**bgp** | **connected** | **isis** [*process-id*] | **ospf** *process-id* | **static**] [**vrf** *vrf-name*]

Parameter Description

bgp: Displays the redistributed BGP route.

connected: Displays the redistributed direct route.

isis *process-id*: Displays the redistributed IS-IS route. Here, *process-id* indicates the IS-IS process ID.

ospf *process-id*: Displays the redistributed OSPF route. Here, *process-id* indicates the OSPF process ID. The value range is from 1 to 65535.

static: Displays the redistributed static route.

vrf *vrf-name*: Specifies a VRF.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information about external routes redistributed by RIP.

```
Hostname> enable
Hostname# show ip rip external
Protocol connected route:
[connected] 192.100.3.0/24 metric=0
    nhop=0.0.0.0, if=2
 [connected] 192.101.1.0/24 metric=0
    nhop=0.0.0.0, if=3
Protocol static route:
 [static] 10.1.1.1/32 metric=0
    nhop=0.0.0.0, if=4096
 [static] 10.1.2.1/32 metric=0
    nhop=0.0.0.0, if=4096
Protocol ospf 1 route:
 [ospf] 1.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
 [ospf] 90.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
```

Table 1-3 Output Fields of the show ip rip external Command

Field	Description
Protocol connected route	Indicates the type of the redistributed route.
connected	Indicates the redistributed route.
metric	Indicates the metric of the redistributed route.
nhop	Indicates the next hop of the redistributed route.
if	Indicates the outbound interface of the redistributed route.

Notifications

14

Platform Description

N/A

Related Commands

N/A

1.38 show ip rip interface

Function

Run the **show ip rip interface** command to display the information about a RIP interface.

Syntax

show ip rip interface [**vrf** *vrf-name*] [*interface-type interface-number*]

Parameter Description

vrf *vrf-name*: Specifies the VRF whose RIP interface is to be displayed.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the information about a RIP interface. If there is no RIP interface, no information will be displayed.

Examples

The following example displays the information about a RIP interface.

```
Hostname> enable
Hostname# show ip rip interface
GigabitEthernet 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:
Not Configured
Authentication mode: Text
Authentication key-chain: ripk1
```

```
Authentication text-password: pswdtext
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
2.2.1.1/24, next update due in 24 seconds
   neighbor 2.2.1.6, next update due in 3 seconds
   neighbor 2.2.1.77, next update due in 13 seconds
2.2.2.57/24, next update due in 16 seconds
```

The following example displays the information about a RIP interface. If RIP correlation with BFD is enabled, BFD information will be also displayed.

```
Hostname> enable
Hostname#show ip rip interface
GigabitEthernet 0/1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 packets only
    Receive RIP packet: Enabled
    Send RIP packet: Enabled
    Send RIP supernet routes: Enabled
    Recv RIP packet total: 0
    Send RIP packet total: 3
    Passive interface: Disabled
Split Horizon: Enabled
Triggered RIP Disabled
BFD: Enabled
    V2 Broadcast: Disabled
    Multicast registe: Registed
    Interface Summary Rip:
      Not Configured
    IP interface address:
      2.2.2.111/24, next update due in 14 seconds
```

Table 1-4 Output Fields of the show ip rip interface Command

Field	Description
Receive RIPv1 and RIPv2 packets	Indicates the type of packets that can be received by an interface.
Send RIPv1 packets only	Indicates the type of packets that can be sent by an interface.
Receive RIP packet	Indicates whether an interface is allowed to receive packets.
Send RIP packet	Indicates whether an interface is allowed to send packets.
Passive interface	Indicates whether a passive interface is enabled.
Send RIP supernet routes	Indicates whether an interface is allowed to send supernetting routes.
Recv RIP packet total	Indicates the total of packets received by an interface.

Field	Description
Send RIP packet total	Indicates the total of packets sent by an interface.
Split Horizon with Poisoned Reverse	Indicates whether split horizon with poison reverse is enabled.
Triggered RIP	Indicates whether the Triggered function is enabled.
Retransmit-timer	Indicates the time of retransmission.
Retransmit-count	Indicates the retransmission count.
V2 Broadcast	Indicates the V2 broadcast packet.
Multicast register	Indicates whether multicast is registered.
Interface Summary Rip	Indicates whether summarization is enabled on an interface.
Authentication mode	Indicates the authorization mode.
Authentication key-chain	Indicates the key-chain used for authentication.
Authentication text-password	Indicates the authentication character string.
Default-information	Indicates the default metric, default route, and other information.
IP interface address	Indicates the IP address of an interface.
BFD	Indicates whether the BFD function is enabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.39 show ip rip peer

Function

Run the **show ip rip peer** command to display the information about a RIP neighbor.

Syntax

show ip rip peer [*ipv4-address*] [**vrf** *vrf-name*]

Parameter Description

ipv4-address: Address of the specified RIP neighbor.

vrf *vrf-name*: Specifies the VRF whose RIP interface is to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

RIP records the summary information for the information source (the source address of the RIP route update packet) of the learned RIP route to realize convenient monitoring by users. These routing information sources are called RIP neighbor information.

This command is used to display the information about a RIP neighbor. If there is no RIP neighbor, no information will be displayed.

Examples

The following example displays the information about a RIP neighbor.

```
Hostname> enable
Hostname# show ip rip peer
Peer 192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/2
  Peer version: RIPv1
  Received bad packets: 3
  Received bad routes: 0
  BFD session state up
```

Table 1-5 Output Fields of the show ip rip peer Command

Field	Description
Peer	Indicates the IP address of a neighbor.
Local address	Indicates the local address.
Input interface	Indicates the connected interface.
Peer version	Indicates the RIP version No. of a neighbor.
Received bad packets	Indicates the packets with errors received from a neighbor.
Received bad routes	Indicates the received routes with errors.
BFD session state	Indicates the BFD session state.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.40 timers basic

Function

Run the **timers basic** command to adjust the clock of RIP.

Run the **no** form of this command to restore the default configuration.

By default, the update timer is 30s, the invalid timer is 180s, the flush timer is 120s, and the holddown timer is 0s.

Syntax

timers basic *update invalid flush* [**holddown** *holddown*]

no timers basic

Parameter Description

update: Interval at which the device sends the route update packet, in seconds. Each time an update packet is received, the invalid timer and flush timer are reset. The value range is from 0 to 2147483647.

invalid: Time after which a route in the routing table becomes invalid because the route is not updated, in seconds. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If a route update packet is received before the invalid timer expires, the timer is reset. The value range is from 0 to 2147483647.

flush: Route flushing time, in seconds, counted from the time when the RIP route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The value range is from 0 to 2147483647.

holddown *holddown*: Specifies the route holddown time, in seconds, counted from the time when the RIP route enters the invalid state. Within the holddown time, the RIP route can only be updated using the routes that come from the same neighbor and have a metric less than 16. The value range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Adjusting the above timers may reduce the convergence time and failback time of the routing protocol. For routers connected to the same network, values of the three RIP timers must be the same. Generally, you are not advised to modify the RIP timers unless otherwise required.

You can run the **show ip rip** command to display the current parameter settings of RIP timers.

Note

Setting timers to small values on a low-speed link brings risks because a lot of Update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

Examples

The following example configures to send RIP update packets every 10s. If no update packet is received within 30s, the corresponding route will become invalid and enter the invalid state. After entering the invalid state for more than 90s, the route will be deleted from the routing table.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# timers basic 10 30 90
```

Notifications

N/A

Common Errors

The RIP process update time and other settings are inconsistent on different devices.

Platform Description

N/A

Related Commands

- **show ip rip**

1.41 validate-update-source

Function

Run the **validate-update-source** command to validate the source address of a received RIP route update packet.

Run the **no** form of this command to disable source address validation for update packets.

The source address validation function for update packets is enabled by default.

Syntax

validate-update-source

no validate-update-source

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can run the command to validate the source address of a RIP route update packet. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor. Two special cases are as follows:

- After split horizon is disabled on an interface, the RIP routing process will perform source address validation on the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an interface not configured with an IP address, the RIP routing process does not perform source address validation for the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.

Examples

The following example disables source address validation of update packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# no validate-update-source
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 version

Function

Run the **version** command to configure the RIP version No. of the entire device.

Run the **no** form of this command to restore the default configuration.

By default, route update packets of RIPv1 and RIPv2 can be received, but only route update packets of RIPv1 are sent.

Syntax

version { **1** | **2** }

no version

Parameter Description

1: Defines the RIP version No. as 1.

2: Defines the RIP version No. as 2.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can run the **ip rip receive version** and **ip rip send version** commands to redefine the specific version of RIP packets to be processed by each interface.

Examples

The following example sets the RIP version No. of the entire device to **2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# version 2
```

Notifications

N/A

Common Errors

The local RIP instance is set to version 1, while the peer sends packets of version 2, leading to a parsing failure.

Platform Description

N/A

Related Commands

- **show ip rip**

1 RIPng Commands

Command	Function
clear ipv6 rip	Delete Routing Information Protocol next generation (RIPng) routes.
default-metric	Define the default metric of RIPng when routes are redistributed using other routing protocols.
distance	Configure the management distance of RIPng routes.
distribute-list	Configure and use a prefix list to filter the inbound/outbound update routes.
graceful-restart	Configure the RIPng graceful restart (GR) function of a device.
ipv6 rip default-information	Configure and generate a default IPv6 path to RIPng.
ipv6 rip enable	Enable RIPng on an interface.
ipv6 rip metric-offset	Configure the metric on an interface.
ipv6 rip subvlan	Enable the RIPng function on a super VLAN.
ipv6 router rip	Create a RIPng routing process and enter routing process configuration mode.
passive-interface	Prohibit an interface from sending RIPng update packets.
redistribute	Configure to redistribute the paths of other routing domains to RIPng.
show ipv6 rip	Display the parameters and all the statistics of a RIPng routing protocol process.
show ipv6 rip database	Display the entry information of a RIPng routing table.
split-horizon	Enable the split horizon function of RIPng.
timers	Configure and adjust the timers of RIPng.

1.1 clear ipv6 rip

Function

Run the **clear ipv6 rip** command to delete Routing Information Protocol next generation (RIPng) routes.

Syntax

clear ipv6 rip

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Running this command deletes all the routes sent by RIPng, which may cause service interruption.

Examples

The following command deletes RIPng routes.

```
Hostname> enable
Hostname# clear ipv6 rip
```

Notifications

N/A

Platform Description

N/A

1.2 default-metric

Function

Run the **default-metric** command to define the default metric of RIPng when routes are redistributed using other routing protocols.

Run the **no** form of this command to restore the default configuration.

By default, the metric for route redistribution is 1.

Syntax

default-metric *metric*

no default-metric

Parameter Description

metric-value: Default metric value. The value range is from 1 to 16. If the value of *metric-value* is equal to or greater than 16, the device determines that this route is unreachable.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command must be used together with the **redistribute** command. When a route is redistributed from another routing protocol process to the RIP route process, the route metric cannot be converted because the metric calculating mechanism is different for each routing protocol. Therefore, in the process of transformation, you need to define the metric of redistributed route in the RIP routing domain. If the metric is not specified during redistribution of a routing protocol process, RIP uses the metric defined by the **default-metric** command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric. If this command is not configured, the metric value is **1** by default.

Examples

The following example sets the default metric value of RIPng to **3** when OSPF 100 is redistributed.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# default-metric 3
Hostname(config-router)# redistribute ospf 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip database**

1.3 distance

Function

Run the **distance** command to configure the management distance of RIPng routes.

Run the **no** form of this command to restore the default configuration.

The management distance is **120** by default.

Syntax

distance *distance*

no distance

Parameter Description

distance: Management distance of RIPng routes. The value range is from 1 to 255.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This function is used to set the management distance of RIP routes and change the priority of a device in routing.

Examples

The following example sets the management distance of RIPng routes to **160**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config)# ipv6 router rip
Hostname(config-router)# distance 160
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.4 distribute-list

Function

Run the **distribute-list** command to configure and use a prefix list to filter the inbound/outbound update routes.

Run the **no** form of this command to cancel the corresponding filtering process.

By default, the distribution list is disabled.

Syntax

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-number*]

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-number*]

Parameter Description

prefix-list *prefix-list-name*: Specifies the name of the prefix list, which is used to filter routes.

in | **out**: Specifies update routes (received or sent routes) that are filtered.

interface-type interface-number: Interface for which the distribution list will be used.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To refuse receiving or sending some specified routes, you can configure a route distribution control list to filter all the route update packets. If no interface is specified, route update packets on all interfaces will be filtered.

Examples

The following example configures and uses the prefix list allowpre to filter the update routes received by the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config)# ipv6 router rip
Hostname(config-router)# distribute-list prefix-list allowpre in GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 graceful-restart

Function

Run the **graceful-restart** command to configure the RIPng graceful restart (GR) function of a device.

Run the **no** form of this command to restore the default configuration.

The GR function is enabled by default.

Syntax

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

graceful-restart: Enables the GR function.

grace-period *grace-period*: Specifies the GR period, in seconds. The value range is 1 to 1800. The default value is twice the update time or 60s, whichever is the smaller.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The GR function is configured based on RIPng instances. You can configure different parameters for different RIPng instances based on the actual conditions.

The GR period is the maximum time from restart of the RIPng process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIPng route is restored so as to restore the RIPng state before the restart. After the restart period expires, RIPng exits the GR state and performs common RIPng operations.

The **graceful-restart grace-period** command allows you to explicitly modify the GR period. Note that GR must be completed before the invalid timer of the RIPng route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are not advised to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalid timer based on the configuration of the **timers** command.

During the RIPng GR process, ensure that the network environment is stable.

Examples

The following example configures the RIPng GR function of a device, and sets the GR period to 90s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# graceful-restart grace-period 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.6 ipv6 rip default-information

Function

Run the **ipv6 rip default-information** command to configure and generate a default IPv6 path to RIPng.

Run the **no** form of this command to delete the default IPv6 path.

By default, default route advertisement is disabled on an interface.

Syntax

ipv6 rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ipv6 rip default-information

Parameter Description

only: Advertises only the IPv6 default route.

originate: Advertises the IPv6 default route and other routes.

metric *metric-value*: Specifies the metric of the default route. The value range is from 1 to 15, and the default value is **1**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to introduce the default route to an autonomous system (AS) edge device so that other devices in the RIPng domain access other AS domains through this AS edge device by default. In the routing table, a route to the destination network ::/0 is called default route. The default route can be learned from a neighbor device, or sent to a neighbor device. Please configure and distribute the default route according to the actual situation of networking, or specify the cost of the distributed default route.

After this command is configured on the interface, an IPv6 default route is advertised to the external devices through this interface, but the route itself is not added to the route forwarding table or the device and the RIPng route database.

To prevent occurrence of a route loop, once this command is configured on an interface, RIPng refuses to receive the default route updates advertised by neighbors.

Examples

The following example configures to generate a default IPv6 route to RIPng on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 rip default-information only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.7 ipv6 rip enable

Function

Run the **ipv6 rip enable** command to enable RIPng on an interface.

Run the **no** form of this command to disable RIPng on a specified interface.

By default, an interface is not added to the RIPng process.

Syntax

ipv6 rip enable

no ipv6 rip enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to set an interface participating in the running of RIPng. If RIPng is not running before the command is configured, configuring the command automatically runs the RIPng routing protocol.

Examples

The following example enables RIPng on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 rip enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.8 ipv6 rip metric-offset

Function

Run the **ipv6 rip metric-offset** command to configure the metric on an interface.

Run the **no** form of this command to cancel the corresponding configuration.

By default, the metric on an interface is **1**.

Syntax

ipv6 rip metric-offset *metric*

no ipv6 rip metric-offset

Parameter Description

metric: Metric on an interface. The value range is from 1 to 16.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

Examples

The following example sets the metric on the GigabitEthernet 0/1 interface to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 rip metric-offset 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.9 ipv6 rip subvlan

Function

Run the **ipv6 rip subvlan** command to enable the RIPng function on a super VLAN.

Run the **no** form of this command to restore the default configuration.

By default, the RIPng function is disabled on a super VLAN.

Syntax

ipv6 rip subvlan [**all** | *vid*]

no ipv6 rip subvlan

Parameter Description

all: Allows sending packets to all sub VLANs.

vid: Sub VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIP multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIP multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the RIPng function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets need to

be sent to only one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. You can run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the RIPng function on Super VLAN 300 and allows sending packets to Sub VLAN 1024.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# ipv6 rip subvlan 1024
```

Notifications

N/A

Common Errors

The function is configured on a non-super VLAN.

The specified sub VLAN on the super VLAN cannot implement interworking with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 router rip

Function

Run the **ipv6 router rip** command to create a RIPng routing process and enter routing process configuration mode.

Run the **no** form of this command to delete the RIPng routing process.

The RIPng routing process is disabled by default.

Syntax

ipv6 router rip

no ipv6 router rip

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to create a RIPng routing process and enter routing process configuration mode.

Examples

The following example creates a RIPng routing process and enters routing process configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
```

Notifications

When the IPv6 unicast function is not enabled and you cannot configure this command, the following notification will be displayed:

```
IPv6 unicast-routing not enabled, RIPng process can't configure
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.11 passive-interface

Function

Run the **passive-interface** command to prohibit an interface from sending RIPng update packets.

Run the **no** form of this command to re-enable the function of sending RIPng update packets.

By default, a RIPng-enabled interface is allowed to send and receive RIPng update packets normally.

Syntax

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

default: Sets all the interfaces to passive mode.

interface-type interface-num: Interface type and interface number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

A passive interface is set with the boundary of RIPng routing domain. The network segment of the passive interface belongs to the RIPng routing domain, but RIPng packets cannot be sent over the passive interface.

The interface set to a passive interface suppresses RIP update packets. A passive interface defines the boundary of RIP routing domain to avoid unwanted flooding of RIP packets. If the interface connection device does not run the RIP routing protocol (such as a PC and a device running other routing protocols), you are advised to configure this interface as a passive interface.

If RIPng routes need to be exchanged on an interface (such as the device interconnection interface) in the RIPng routing domain, this interface cannot be configured as a passive interface.

Examples

The following example sets all interfaces to passive mode, and enables the function of sending update packets on the Gigabit Ethernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface GigabitEthernet 0/1
```

Notifications

When the configured interface is invalid or does not exist, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 redistribute

Function

Run the **redistribute** command to configure to redistribute the paths of other routing domains to RIPng.

Run the **no** form of this command to cancel the corresponding redistribution configuration.

The redistribution function is not configured by default. This function redistributes the routes of all subtypes of the specified routing process.

Syntax

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** | **route-map**] *

Parameter Description

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

isis [*area-tag*]: Indicates redistribution from IS-IS. *area-tag* indicates the IS-IS process ID.

ospf *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value range is from 1 to 65535.

static: Indicates redistribution from static routes.

metric *metric-value*: Sets the metric of the route redistributed to the RIPng domain. The value range is from 1 to 16, and the default value is **1**.

route-map *route-map-name*: Indicates the associated route map, which is used to set the redistribution filtering rules.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

RIPng can distribute the routes of other routing protocols in the local routing domain so that the devices in the routing domain can access other routing domains.

During route redistribution, different routing protocols use different metric measurement methods. For example, RIPng measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, however, it is necessary to configure a symbolic metric; otherwise, route redistribution fails.

Examples

The following example configures redistributing the static routes satisfying the route map mymap into RIPng.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# redistribute static route-map mymap metric 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip database**

1.13 show ipv6 rip

Function

Run the **show ipv6 rip** command to display the parameters and all the statistics of a RIPng routing protocol process.

Syntax

show ipv6 rip

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The command can be used to quickly display the three timers, route distribution, route redistribution status, RIPng version of interface, RIPng interface, network scope, metric, management distance, and other information of a RIPng routing protocol process.

Examples

The following example displays the parameters and all the statistics of a RIPng routing protocol process.

```
Hostname> enable
Hostname# show ipv6 rip
Routing Protocol is "RIPng"
  Sending updates every 10 seconds with +/-50%, next due in 8 seconds
  Timeout after 30 seconds, garbage collect after 60 seconds
  Outgoing update filter list for all interface is:
    distribute-list prefix aa out
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 1
  Distance: 120 (default is 120)  Redistribution:
     Redistributing protocol connected route-map rm
     Redistributing protocol static
     Redistributing protocol ospf 1
  Default version control:  send version 1, receive version 1
```

```
 Interface              Send   Recv
    VLAN 1             1      1
    Loopback 1          1      1
 Routing Information Sources:
    None
```

Table 1-1 Output Fields of the show ipv6 rip Command

Field	Description
Sending update	Indicates the interval for sending update packets.
Sending update	Indicates the failure time.
garbage	Indicates the recovery time.
Outgoing update filter list	Indicates the configured filter table of sent packets.
Incoming update filter	Indicates the configured filter table of received packets.
Default redistribution metric	Indicates the default redistribution metric.
distance	Indicates the management distance.
Redistribution	Indicates the redistribution routing protocol.
Default version control	Indicates the default RIPng version No. received/sent.
Interface	Indicates the interface that joins the RIPng process.
Routing Information Sources:	Routing Info

Notifications

N/A

Platform Description

N/A

1.14 show ipv6 rip database

Function

Run the **show ipv6 rip database** command to display the entry information of a RIPng routing table.

Syntax

show ipv6 rip database

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the information of each entry in the RIPng routing table.

Examples

The following example displays the information of each entry in the RIPng routing table.

```
Hostname# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
         i - interface, a/s - aggregated/suppressed
S(r)   2001:db8:1::/64, metric 1, tag 0
         Loopback 0/::
S(r)   2001:db8:2::/64, metric 1, tag 0
         Loopback 0/::
C(r)   2001:db8:3::/64, metric 1, tag 0
         VLAN 1/::
S(r)   2001:db8:4::/64, metric 1, tag 0
         Null 0/::
C(i)   2001:db8:5::/64, metric 1, tag 0
         Loopback 1/::
S(r)   2001:db8:6::/64, metric 1, tag 0
         Null 0/::
```

Table 1-2 Output Fields of the show ipv6 rip database Command

Field	Description
codes	Indicates the route type and corresponding abbreviation description.
2001:db8:1::	Indicates the corresponding prefix of the route.
metric 1	Indicates the corresponding metric of the route.
VLAN 1/::	Indicates the route interface.

Notifications

N/A

Platform Description

N/A

1.15 split-horizon

Function

Run the **split-horizon** command to enable the split horizon function of RIPng.

Run the **split-horizon poisoned-reverse** command to enable split horizon with poison reverse.

Run the **no** form of this command to disable split horizon with poison reverse.

By default, the split horizon function without poison reverse is enabled on an interface.

Syntax

split-horizon

split-horizon poisoned-reverse

no split-horizon poisoned-reverse

Parameter Description

poisoned-reverse: Enables split horizon with poison reverse.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In update packets, the split horizon function can prevent a device from advertising some routing information from the interface that has learned the routing information. The split horizon with poison reverse advertises some routing information from the interface that has learned the routing information, but sets the corresponding metric value to **16**.

The RIPng routing protocol falls into distance vector routing protocols, so the problem of split horizon must be noted in the actual application. If you cannot determine whether split horizon has been enabled for RIPng, you can run the **show ipv6 rip** command to make judgment.

Examples

The following example disables split horizon of RIPng.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# no split-horizon
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1.16 timers

Function

Run the **timers** command to configure and adjust the timers of RIPng.

Run the **no** form of this command to restore the default configuration.

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Syntax

timers *update invalid flush*

no timers

Parameter Description

update: Route update time, in seconds. The parameter defines the interval at which a device sends route update packets. Each time an update packet is received, the invalid timer and flush timer are reset. The value range is from 0 to 2147483647.

invalid: Route invalid time, in seconds, counted from the last time when a valid update packet is received. The *invalid* parameter defines the time after which a route in the routing table becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If a route update packet is received within the time of *invalid*, the timer is reset. The value range is from 0 to 2147483647.

flush: Route flushing time, in seconds, counted from the time when the RIPng route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The value range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Adjusting the above timers may reduce the convergence time and failback time of the routing protocol. For devices connected to the same network, values of the three RIPng timers must be the same. Generally, you are not advised to modify the RIP timers unless otherwise required.

You can run the **show ipv6 rip** command to display the current parameter settings of RIPng timers.

Note

Setting timers to small values on a low-speed link brings risks because a lot of Update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

Examples

The following example configures to send RIP update packets every 10s. If no update packet is received within 30s, the corresponding route will become invalid and enter the invalid state. After entering the invalid state for more than 90s, the route will be deleted from the routing table.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router rip
Hostname(config-router)# timers 10 30 90
```

Notifications

N/A

Common Errors

Different RIPng timers are configured on different devices. Consequently, routes cannot be learned properly.

Platform Description

N/A

Related Commands

- **show ipv6 rip**

1 OSPFv2 Commands

Command	Function
area	Configure a specified open shortest path first (OSPF) area.
area authentication	Enable OSPF area authentication.
area default-cost	Configure the cost advertised to the default route of a stub area or not-so-stubby area (NSSA).
area filter-list	Configure the filtering conditions of inter-area route learning.
area nssa	Configure an OSPF area as NSSA.
area range	Configure route summarization between OSPF areas.
area stub	Set an OSPF area to a stub or totally stub area.
area sham-link	Configure a sham link.
area virtual-link	Configure an OSPF virtual link.
asbr enable	Enable a device as an ASBR.
auto-cost	Configure the reference value of interface cost.
bfd all-interfaces	Configure link detection through bidirectional forwarding detection (BFD) for all the interfaces running OSPF.
capability opaque	Enable the opaque LSA processing capability.
capability vrf-lite	Forcibly disable the automatic judging function of support to loop detection for OSPF processes.
clear ip ospf process	Clear and restart an OSPF process.
compatible rfc1583	Enable the RFC1583 rules.
default-information originate	Generate a default route to be injected to the OSPF routing domain.
default-metric	Configure the default metric for an OSPF redistributed route.
disable-dn-bit-check	Disable the DN bit loop detection function of LSA.

disable-tag-check	Disable loop detection using the route tag of LSA.
discard-route	Allow adding a discard route to the core routing table.
distance	Configure the management distances corresponding to different types of OSPF routes.
distribute-list in	Configure filtering routes that are calculated based on the received LSA.
distribute-list out	Configure filtering of redistributed routes.
domain-id	Configure the domain ID of an OSPF process.
domain-tag	Configure the VPN route tag of an OSPF process associated with VRF.
enable mib-binding	Bind the MIB to a specified OSPFv2 process.
enable traps	Enable sending of the specified trap message.
extcommunity-type	Configure the Router-ID or Route-Type of an OSPF process associated with VRF.
fast-reroute	Configure the OSPF fast reroute function of a device.
graceful-restart	Enable the OSPF GR capability and set the GR period.
graceful-restart helper	Enable the OSPF GR helper function and configure the relevant topology change detection mode.
ip ospf authentication	Configure the authentication mode of an interface.
ip ospf authentication-key	Configure the plain text authentication key of OSPF.
ip ospf area	Configure an OSPF routing process in which an interface participates.
ip ospf bfd	Configure an OSPF-enabled interface to enable or disable the BFD function.
ip ospf cost	Configure the cost value for an OSPF interface to send a packet.
ip ospf cost-fallback	Configure the cost fallback of an aggregation port (AP).
ip ospf database-filter all out	Prevent an interface from diffusing LSA packets to the outside, that is, LSA update packets are not sent from the interface.

ip ospf dead-interval	Configure the interval for OSPF to determine the failure of a specified interface neighbor.
ip ospf disable all	Prevent a specified interface from generating OSPF packets.
ip ospf fast-reroute protection	Enable the loop-free alternate (LFA) protection mode of a specified interface.
ip ospf fast-reroute no-eligible-backup	Exclude an OSPF interface that cannot be used as a backup interface in the OSPF fast reroute calculation.
ip ospf hello-interval	Configure the interval for OSPF to send hello packets.
ip ospf message-digest-key	Configure a cipher text authentication key of OSPF packets.
ip ospf mtu-ignore	Disable MTU verification when an interface receives database description packets.
ip ospf network	Configure the OSPF network type of an interface.
ip ospf priority	Configure the OSPF priority value of an interface.
ip ospf retransmit-interval	Configure the retransmission interval of LSU packets on an interface.
ip ospf source-check-ignore	Disable the source address verification function for the packets received on a P2P link.
ip ospf subvlan	Enable the OSPF function on a super VLAN.
ip ospf transmit-delay	Configure the delay for an OSPF interface to transmit LSU packets.
ispf enable	Enable the incremental shortest path first (iSPF) feature and run the iSPF algorithm to calculate the network topology.
log-adj-changes	Record the log of adjacency state changes.
max-concurrent-dd	Configure the maximum number of neighbors with which the current OSPF process can concurrently initiate or accept interaction.
max-metric router-lsa	Configure the maximum advertisement metric of an OSPF-enabled device so that other routers will not preferably regard this router as a transmission node in SPF calculation.

neighbor	Configure an OSPF neighbor.
network area	Configure which interfaces will run OSPF and which OSPF area they belong to.
nsr	Configure the current OSPF process to support the non-stop routing (NSR) function.
overflow database	Configure the maximum number of LSAs supported by the current OSPF process.
overflow database external	Configure the maximum number of external LSAs and the waiting time for recovery from the overflow state to the normal state.
overflow memory-lack	Allow the OSPF process to enter the overflow state when the memory is insufficient.
passive-interface	Configure a network interface specified for the local router as a passive interface.
redistribute	Enable the function of redistributing the external routing information.
router ospf	Create an OSPF routing process and enter routing configuration mode of OSPF.
router ospf max-concurrent-dd	Configure the maximum number of neighbors with which all the OSPF routing processes can concurrently initiate or accept interaction.
router-id	Configure the ID of a router.
show ip ospf	Display the summary of an OSPF process.
show ip ospf border-routers	Display the OSPF internal routing table to an ABR/ASBR.
show ip ospf database	Display the information of an OSPF LSDB.
show ip ospf interface	Display the information about an interface associated with an OSPF process.
show ip ospf ispf	Display the times of route computation through iSPF in the OSPF area.
show ip ospf neighbor	Display the neighbor table of an OSPF process.
show ip ospf route	Display an OSPF route.
show ip ospf sham-links	Display the sham link information of an OSPF process.

show ip ospf spf	Display the times of route computation in the OSPF area.
show ip ospf summary-address	Display the summarized route of all the redistributed routes of an OSPF process.
show ip ospf topology	Display the topology information of SPF computation of an OSPF process.
show ip ospf virtual-links	Display the information about a virtual link of an OSPF process.
show running-config router ospf	Display the configuration of an OSPF process.
summary-address	Configure a summarized route for the external routes of the OSPF routing domain.
timers lsa arrival	Configure the delay for receiving a duplicate LSA.
timers pacing lsa-group	Configure a group pacing interval of LSA.
timers pacing lsa-transmit	Configure an interval for sending LSA group and a number of LS-UPD packets in each group.
timers spf	Configure the delay time for SPF computation after an OSPF process receives the topology change information and the time interval between two SPF computations.
timers throttle lsa all	Configure an exponential backoff algorithm of LSA packet generation.
timers throttle route	Configure the delay time for route computation when an OSPF process receives changed inter-area and external LSAs.
timers throttle spf	Configure the delay time for SPF computation, and the minimum interval and maximum interval for two SPF computations after an OSPF process receives the topology change information.
two-way-maintain	Enable the two-way maintenance function of an OSPF process.

1.1 area

Function

Run the **area** command to configure a specified open shortest path first (OSPF) area.

Run the **no** form of this command to delete a specified OSPF area.

No OSPF area is configured by default.

Syntax

area *area-id*

no area *area-id*

Parameter Description

area-id: OSPF area ID. The parameter can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can run the **no** form of this command to clear the configuration of a specified OSPF area and delete this area, including the configurations of the area-based commands such as **area authentication**, **area default-cost**, **area filter-list**, and **area nssa**.

You cannot clear the configuration of the OSPF area in the following cases:

- All the configuration of the backbone area needs to be cleared, but there is a virtual link configuration. In this case, the virtual link configuration must be cleared before the backbone area can be deleted.
- There is a corresponding **network area** command in all the areas. In this case, you must clear all the network segment commands that are added to the area before deleting the area.

Examples

The following example deletes the related configuration of OSPF area 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 2
Hostname(config-router)# no area 2
```

Notifications

When you delete the **area** configuration without deleting the **network** command, the following notification will be displayed.

```
% Error: Area 1 cannot be deleted before its network command is removed
```

Common Errors

You want to delete the **area** configuration without deleting the **network** command.

Platform Description

N/A

1.2 area authentication

Function

Run the **area authentication** command to enable OSPF area authentication.

Run the **no** form of this command to disable OSPF area authentication.

The OSPF area authentication function is disabled by default.

Syntax

area *area-id* **authentication** [**message-digest** | **keychain** *name*]

no area *area-id* **authentication**

Parameter Description

Area-id:-id: ID of the area with OSPF authentication to be enabled. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

message-digest: Enables cipher text authentication mode.

keychain *name*: Name of the adopted keychain authentication. If **Keychain** specifies that the authentication type is **SM3**, the key ID value range is from 0 to 255.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The device supports three authentication types:

- Type 0: No authentication is required. When the **area authentication** command is not used to enable OSPF authentication, the authentication type in OSPF data packets is type 0.
- Type 1: The authentication type is plain text authentication mode. In this mode, the **message-digest** parameter is not contained.
- Type 2: The authentication type is cipher text authentication mode. In this mode, the **message-digest** parameter is contained.

All routers in the same OSPF area must run the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors.

- You can run the **ip ospf authentication-key** command on an interface to configure a plain text authentication key.
- You can run the **ip ospf message-digest-key** command on an interface to configure a cipher text

authentication key.

- If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, Message-Digest 5 (MD5) authentication, and SM3 authentication.

Examples

The following example configures MD5 authentication for Area 0 (backbone area) of the OSPF routing process, and sets the authentication key for the interface GigabitEthernet 0/1 connected to neighbors to **backbone**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# router ospf 1
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# area 0 authentication message-digest
```

The following example configures keychain authentication for Area 0 (backbone area) of the OSPF routing process, and sets the keychain name to **ospf**. The configured authentication key for keychain ospf is **hello**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# area 1 authentication keychain ospf
Hostname(config-router)# exit
Hostname(config)# key chain ospf
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string hello
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**
- **ip ospf authentication-key**
- **ip ospf message-digest-key**

1.3 area default-cost

Function

Run the **area default-cost** command to configure the cost advertised to the default route of a stub area or not-so-stubby area (NSSA).

Run the **no** form of this command to restore the default configuration.

By default, the cost value of a route is 1.

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

area-id: ID of a stub area or NSSA. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

cost: Cost of the default route injected to the stub area or NSSA. The value range is from 0 to 16777215.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only on an area border router (ABR) in a stub area or on an ABR/autonomous system boundary router (ASBR) in an NSSA.

An ABR in a stub area or an ABR/ASBR in an NSSA is allowed to advertise a link-state advertisement (LSA) indicating the default route in the stub or NSSA. You can run the **area default-cost** command to modify the cost of the advertised LSA.

Examples

The following example configures the cost value of the OSPF advertised to a stub area as **50**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.255.255 area 0
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 1
Hostname(config-router)# area 1 stub
Hostname(config-router)# area 1 default-cost 50
```

Notifications

When this command is configured in an area other than the stub area or NSSA, the following notification will be displayed:

```
% The area is neither stub, nor NSSA
```

When this command is configured in a backbone area, the following notification will be displayed:

```
% You can't configure default-cost to backbone
```

Common Errors

This command is configured in an area other than the stub area or NSSA.

This command is configured in a backbone area.

Platform Description

N/A

Related Commands

N/A

1.4 area filter-list

Function

Run the **area filter-list** command to configure the filtering conditions of inter-area route learning.

Run the **no** form of this command to cancel this configuration.

By default, the filtering conditions of inter-area route learning are not configured.

Syntax

area *area-id* **filter-list** { **access** *acl-number* | **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-number* | **prefix** *prefix-name* } { **in** | **out** }

Parameter Description

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

access *acl-number*: Associated standard ACL. The value range is from 1 to 99.

prefix *prefix-name*: Name of the associated prefix list. The value is a case-sensitive string of 1 to 99 characters.

in: Filters the routes that are received by the area.

out: Filters the routes that are sent from the area.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command can be configured only on an ABR.

Run this command when it is required to configure filtering conditions for inter-area routes on the ABR.

Examples

The following example configures OSPF Area 1 that is allowed to learn only the inter-area routes within the range of 172.22.0.0/8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 172.22.0.0 0.255.255.255
Hostname(config)# router ospf 100
Hostname(config-router)# area 1 filter-list access 1 in
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 area nssa

Function

Run the **area nssa** command to configure an OSPF area as NSSA.

Run the **no** form of this command to delete this configuration.

The NSSA function is disabled by default.

Syntax

area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** *stability-interval*] *] *

no area *area-id* **nssa** [**default-information-originate** [**metric** *value* | **metric-type** *type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval**] *] *

Parameter Description

area-id: ID of the NSSA, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

default-information-originate: Indicates that a default Type-7 LSA is generated and introduced to the NSSA. This option takes effect only on an NSSA ABR or ASBR.

metric *metric*: Indicates the metric of the generated default LSA. The value range is from 0 to 16777214, and the default value is **1**.

metric-type *metric-type*: Indicates the route type of the generated default LSA. The value is 1 or 2. Here, 1 represents N-1, and 2 represents N-2. The default value is 2.

no-redistribution: When the router is an NSSA ABR and you want to use only the route redistribution command to introduce the routing information into a common area instead of an NSSA, select this option.

no-summary: Prohibits the ABR in the NSSA from sending Summary LSAs (Type-3 LSA).

translator: Indicates that the NSSA ABR is a translator.

always: Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator.

stability-interval *stability-interval*: Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator, in seconds. The value range is 0 to 2147483647, and the default value is **40**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

- The **default-information-originate** parameter is used to generate a default Type-7 LSA. This option is different for the NSSA ABR and ASBR. On ABR, a Type-7 LSA default route is generated regardless of whether there is a default route in the routing table. On ASBR (which is not an ABR at the same time), a Type-7 LSA default route is generated only when there is a default route in the routing table.
- If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be distributed to the NSSA. This parameter is generally used when a router in the NSSA acts both as an ASBR and an ABR. It prevents external routing information from entering the NSSA.
- To further reduce the number of LSAs sent to the NSSA, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the Summary LSAs (Type-3 LSA) to the NSSA.
- When the **translator always** parameter is configured, if an NSSA has two or more area border routers (ABRs), the ABR with the largest router ID is selected by default as the translator for converting Type-7 LSAs into Type-5 LSAs. If the current device is expected to be always the translator ABR for converting Type-7 LSAs into Type-5 LSAs, run the **translator always** parameter. In the same NSSA, it is recommended that this parameter be configured on only one ABR.
- When the **stability-interval** parameter is configured, if the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by *stability-interval*. If the router does not become a translator again within the above time, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after *stability-interval* expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 are deleted from the AS immediately after the current device loses the translator role even if *stability-interval* does not expire.

Examples

The following example sets Area 1 to NSSA.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.255.255 area 0
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 1
Hostname(config-router)# area 1 nssa
```

Notifications

When the backbone area is set to NSSA, the following notification will be displayed:

```
% You can't configure NSSA to backbone
```

Common Errors

The backbone area is set to NSSA.

Platform Description

N/A

Related Commands

- **show ip ospf**
- **area** default-cost

1.6 area range

Function

Run the **area range** command to configure route summarization between OSPF areas.

Run the **no** form of this command to delete this configuration.

By default, no route summarization is configured between OSPF areas.

Syntax

area *area-id* **range** *ipv4-address mask* [**advertise** | **not-advertise**] [**cost** *cost* | **inherit-minimum**]

no area *area-id* **range** *ipv4-address mask* [**cost** | **inherit-minimum**]

Parameter Description

area-id: ID of the OSPF area to which the summarized route will be injected. The parameter can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

ipv4-address mask: Network segment of the summarized route.

advertise: Advertises the summarized route.

not-advertise: Not advertises the summarized route.

cost *cost*: Indicates the metric of the summarized route. The value range is from 0 to 16777215. The default metric of a summarized route is related to compatibility with RFC1583. If the RFC1583 compatibility mode is configured, the default metric is the minimum value of the metric of the summarized route; otherwise, the default metric is the maximum value of the metric of the summarized route. The combination of the **no** prefix and **cost** parameter can restore the default metric of a summarized route, but will not delete route summarization.

inherit-minimum: Sets the minimum value of all the route metrics before summarization to the route metric after summarization.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an area into one route, and advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Although the routers inside the area can learn specific routing information, the routers in other areas can learn only one summarized route. You can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can run the **cost** parameter to set the metric of the summarized route.

You can configure route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improves the network forwarding performance especially for a large-sized network.

When multiple routes for summarization are configured and have the inclusive relationship with each other, the range of routes to be summarized is determined based on the longest match principle.

Examples

The following example summarizes the routes of OSPF Area 1 into 172.16.16.0/20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.15.255 area 0
Hostname(config-router)# network 172.16.17.0 0.0.15.255 area 1
Hostname(config-router)# area 1 range 172.16.16.0 255.255.240.0
```

Notifications

When the summarized route has been configured for different areas, the following notification will be displayed:

```
% OSPF: This range in different area 1
```

Common Errors

The summarized route has been configured for different areas.

Platform Description

N/A

Related Commands

N/A

1.7 area stub

Function

Run the **area stub** command to set an OSPF area to a stub or totally stub area.

Run the **no** form of this command to delete this configuration.

The stub area function is disabled by default.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

area-id: ID of a stub area. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

no-summary: Prohibits the ABR from sending network summary LSAs to the stub. In this case, the stub area can be called a totally stub area. This parameter is configured only when the router is an ABR.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You must run the **area stub** command on all routers in the OSPF stub area. ABR sends only three kinds of LSAs to the stub area:

- Type 1, router LSA.
- Type 2, network LSA.
- Type 3, network summary LSA.

From the perspective of the routing table, a router in the stub area can learn only the internal routes of the OSPF routing domain, including the internal default route generated by an ABR. A router in the stub area cannot learn external routes of the OSPF routing domain.

To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR.

You can run either the **area stub** or **area default-cost** command to configure an OSPF area as a stub area. If **area stub** is used, you must configure this command on all routers connected to the stub area. If **area default-cost** is used, run this command only on the ABR in the stub area. The **area default-cost** command defines the initial cost of the internal default route.

Examples

The following example sets Area 1 to stub area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.255.255 area 0
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 1
Hostname(config-router)# area 1 stub
```

Notifications

When you attempt to configure the backbone area as a stub area, the following notification will be displayed:

```
% You can't configure stub to backbone
```

When you attempt to configure an NSSA as a stub area, the following notification will be displayed:

```
% The area is configured as NSSA area already
```

Common Errors

The backbone area is configured as a stub area.

An NSSA is configure as a stub area.

Platform Description

N/A

Related Commands

- **show ip ospf**
- **area** default-cost

1.8 area sham-link

Function

Run the **area sham-link** command to configure a sham link.

Run the **no** form of this command to delete this configuration.

Run the **default** form of this command to restore the default configuration.

A sham link is disabled by default. No authentication is set for a sham link by default.

Syntax

area *area-id* **sham-link** *source-ipv4-address destination-ipv4-address* [[**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **cost** *number* | **dead-interval** *dead-interval* | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * | **authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

no area *area-id* **sham-link** *source-ipv4-address destination-ipv4-address* [**authentication** | **authentication-key** | **cost** | **dead-interval** | **hello-interval** | **message-digest-key** *key-id* | **retransmit-interval** | **transmit-delay**] *

default area *area-id* **sham-link** *source-ipv4-address destination-ipv4-address* [**authentication** | **authentication-key** | **cost** | **dead-interval** | **hello-interval** | **message-digest-key** *key-id* | **retransmit-interval** | **transmit-delay**] *

Parameter Description

area-id: ID of the OSPF area where the sham link is. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

source-ipv4-address: Source address of the sham link.

destination-ipv4-address: Destination address of the sham link.

authentication: Sets the authentication type to plain text authentication.

keychain *keychain-name*: Sets keychain authentication. If **Keychain** specifies that the authentication type is **SM3**, the key ID value range is from 0 to 255.

message-digest: Sets the authentication type to cipher text authentication.

null: Indicates that authentication is disabled.

cost *number*: Indicates the cost value of the OSPF protocol for sending packets on the sham link. The value range is from 0 to 65535, and the default value is **1**.

dead-interval *dead-interval*: Indicates the dead interval of sham link neighbors, in seconds. The value range is 0 to 2147483647, and the default value is **40**.

hello-interval *hello-interval*: Indicates the time interval of sending hello packets on the sham link, in seconds. The value range is 1 to 65535, and the default value is **10**.

retransmit-interval *retransmit-interval*: Indicates the time interval of packets retransmission on the sham link, in seconds. The value range is 0 to 65535, and the default value is **5**.

transmit-delay *transmit-delay*: Indicates the delay of transmitting link state update (LSU) packets on the sham link, in seconds. The value range is 0 to 65535, and the default value is **1**.

authentication-key [**0** | **7**] *key*: Defines the key for OSPF plain text authentication. The key of plain text authentication must be consistent between neighbors.

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: Key value. The value is a string containing 1–8 characters.

message-digest-key *key-id* [**md5**] [**0** | **7**] *key*: Defines the key ID and key for OSPF cipher text authentication. The key ID and key for cipher text authentication must be consistent between neighbors.

key-id: ID of the authentication key. The value range is from 1 to 255.

md5: Uses the MD5 cipher text authentication.

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: Key value. The value is a string containing 1–8 characters.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only for the OSPF process associated with VPN routing and forwarding (VRF).

A sham link needs to be configured on two provider edges (PEs) for establishing a sham link at the same time. Only one PE cannot establish a sham link.

The **service password-encryption** command makes the key in the command displayed in a way of encryption.

To establish a sham link between two PEs, you must meet the following configuration conditions:

- The *area-id* value of sham link configured for the two PEs must be consistent.
- The combination of source address and destination address of a sham link configured on one PE must be equal to the combination of destination address and source address of a sham link configured on the other PE.
- The source address used to establish a sham link on the PE must be a 32-bit loopback address, and must be bound to the corresponding VRF instance.

Caution

- Since the OSPF route advertised through a sham link has no VPN label, the route cannot be used for forwarding. Actually packets are still forwarded through the Border Gateway Protocol (BGP) VPNv4 route. Therefore, in the actual configuration, you must ensure that the route advertised through the sham link will also be advertised to the corresponding BGP neighbor through Multiprotocol Extensions for BGP (MP-BGP) in the form of VPNv4 route.
- The source address for establishing the sham link must participate in the BGP VPNv4 route advertisement, but cannot join the calculation of VRF OSPF process.

Examples

The following example configures a sham link in OSPF Area 0, with source address 1.1.1.1 and destination address 2.2.2.2, and sets the metric of the packet sent by OSPF on the sham link to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# area 0 sham-link 1.1.1.1 2.2.2.2 cost 10
```

Notifications

N/A

Common Errors

The source address for establishing a sham link joins the calculation of VRF OSPF process.

Only the private route is advertised through the sham link, but the VPNv4 route is not advertised through MP-BGP.

Platform Description

N/A

Related Commands

- **show ip ospf sham-links**

1.9 area virtual-link

Function

Run the **area virtual-link** command to configure an OSPF virtual link.

Run the **no** form of this command to delete this configuration.

No virtual link is configured by default.

Syntax

area *area-id* **virtual-link** *router-id* [**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **dead-interval** { *dead-interval* | **minimal hello-multiplier** *multiplier-time* } | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

no area *area-id* **virtual-link** *router-id* [**authentication** | **authentication-key** | **dead-interval** | **hello-interval** | **message-digest-key** *key-id* | **retransmit-interval** | **transmit-delay**] *

Parameter Description

area-id: ID of the OSPF transit area. The parameter can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

router-id: Router ID for the neighbor of the virtual link. The router ID can be displayed using the **show ip ospf** command.

authentication: Sets the authentication type to plain text authentication.

keychain *keychain-name*: Sets keychain authentication. If **Keychain** specifies that the authentication type is **SM3**, the key ID value range is from 0 to 255.

message-digest: Sets the authentication type to cipher text authentication.

null: Indicates that authentication is disabled.

dead-interval *dead-interval*: Indicates the time that the neighbor is declared lost, in seconds. The value range is 0 to 2147483647, and the default value is **40**. The setting of this parameter must be consistent with that on a neighbor.

minimal hello-multiplier *multiplier-time*: Indicates that the fast hello function is enabled to set the dead interval to 1s. Here, *multiplier-time* indicates the number of hello packets sent per second in the fast hello function. The value range is from 3 to 20. The fast hello function is not enabled by default.

hello-interval *hello-interval*: Indicates the time interval for OSPF to send hello packets on the virtual link, in seconds. The value range is 1 to 65535, and the default value is **10**. The setting of this parameter must be consistent with that on a neighbor.

retransmit-interval *retransmit-interval*: Indicates the OSPF LSA retransmission interval, in seconds. The setting of the time interval should take into account the round trip time of packets on the link. The value range is 0 to 65535, and the default value is **5**.

transmit-delay *transmit-delay*: Indicates the delay after which OSPF sends the LSA, in seconds. This value increases the time to live (TTL) of LSA. When the TTL of LSA reaches the fixed time, the LSA will be refreshed. The value range is 0 to 65535, and the default value is **1**.

authentication-key [**0** | **7**] *key*: Defines the key for OSPF plain text authentication. The key of plain text authentication must be consistent between neighbors.

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: Key value. The value is a string containing 1–8 characters.

message-digest-key *key-id* [**md5**] [**0** | **7**] *key*: Defines the key ID and key for OSPF cipher text authentication.

key-id: ID of the authentication key. The value range is from 1 to 255.

md5: Uses the MD5 cipher text authentication.

The **service password-encryption** command makes the key displayed in a way of encryption.

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: Key value. The value is a string containing 1–8 characters.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In the OSPF routing domain, all the areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA area cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas.

Here, *router-id* is the ID of an OSPF neighbor router. If you are sure about the value of *router-id*, run the **show ip ospf neighbor** command to confirm the value. You can configure the loopback address as the router ID.

The **area virtual-link** command defines only the authentication key of the virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, you must run the **area authentication** command. The **service password-encryption** command makes the key in the command displayed in a way of encryption.

OSPF supports the fast hello function.

- After the OSPF fast hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF fast hello function by specifying the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter. The **minimal** keyword indicates that the dead interval is set to 1s, and **hello-multiplier** indicates the number of hello packets sent per second. In this way, the interval at which the hello packet is sent decreases to less than 1s.
- If the fast hello function is configured for a virtual link, the hello interval field of the hello packet advertised on the virtual link is set to 0, and the hello interval field of the hello packet received on this virtual link is ignored.
- No matter whether the fast hello function is enabled, the dead interval must be consistent and the **hello-multiplier** value can be inconsistent on routers at both ends of the virtual link. Ensure that at least one hello packet can be received within the dead interval.
- Run the **show ip ospf virtual-links** command to monitor the dead interval and the fast hello interval configured for the virtual link.
- The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the fast hello function cannot be configured simultaneously.

Examples

The following example configures Area 1 as a transit area, and establishes a virtual link with neighbor 2.2.2.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.15.255 area 0
Hostname(config-router)# network 172.16.17.0 0.0.15.255 area 1
Hostname(config-router)# area 1 virtual-link 2.2.2.2
```

The following example configures Area 1 as a transit area, and establishes a virtual link with neighbor 1.1.1.1. The virtual link connects Area 10 to the backbone area. The virtual link adopts OSPF packet authentication in authentication mode MD5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.17.0 0.0.15.255 area 1
Hostname(config-router)# network 172.16.252.0 0.0.0.255 area 10
Hostname(config-router)# area 0 authentication message-digest
Hostname(config-router)# area 1 virtual-link 1.1.1.1 message-digest-key 1 md5 hello
```

The following example configures Area 1 as a transit area, establishes a virtual link with neighbor 1.1.1.1, enables the fast hello function on the virtual link, and sets the multiplier to **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.17.0 0.0.15.255 area 1
Hostname(config-router)# network 172.16.252.0 0.0.0.255 area 10
Hostname(config-router)# area 1 virtual-link 1.1.1.1 dead-interval minimal
hello-multiplier 3
```

Notifications

When a virtual link is configured in the backbone area, the following notification will be displayed:

```
% You can't configure virtual-link transit to backbone
```

When a virtual link is configured in a stub area or NSSA, the following notification will be displayed:

```
% Area is a stub or nssa so virtual links are not allowed
```

Common Errors

A virtual link is configured in the backbone area.

A virtual link is configured in a stub area or NSSA area.

Platform Description

N/A

Related Commands

- **area authentication**
- **show ip ospf neighbor**
- **show ip ospf virtual-links**

1.10 asbr enable

Function

Run the **asbr enable** command to enable a device as an ASBR.

Run the **no** form of this command to restore the default value.

ASBR is disabled by default.

Syntax

asbr enable

no asbr enable

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

After the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, configure the **asbr enable** command. If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command is still configured, the device is still ASBR**.**

Examples

The following example enables a device as an ASBR.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# asbr enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf database**

1.11 auto-cost

Function

Run the **auto-cost** command to configure the reference value of interface cost.

Run the **no** form of this command to restore the default value.

By default, the reference bandwidth value of interface cost calculation is 100 Mbps.

Syntax

auto-cost reference-bandwidth *ref-bw*

no auto-cost reference-bandwidth

Parameter Description

ref-bw: Reference bandwidth value, in mega-bytes per second. The value range is from 1 to 4294967.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

By default, the cost of an OSPF interface is equal to the reference value of the interface bandwidth divided by the actual interface bandwidth. When OSPF is allowed on a link above 100 Mbps, you are advised to increase the *ref-bw* value.

Run the **bandwidth** command to set the interface bandwidth.

The default costs of OSPF interfaces on several typical lines are as follows:

- For the 64 Kbps serial line, the cost is 1562.
- For the E1 line, the cost is 48.
- For the 10 Mbps Ethernet, the cost is 10.
- For the 100 Mbps Ethernet, the cost is 1.

If an interface cost is set using the **ip ospf cost** command, the automatically calculated interface cost will be overwritten.

Examples

The following example configures the reference value of interface bandwidth for the automatically calculated interface cost as 10 Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.10.0 0.0.0.255 area 0
Hostname(config-router)# auto-cost reference-bandwidth 10
```

Notifications

When the interface cost is changed, the following notification will be displayed:

```
% OSPF: Reference bandwidth is changed.
       Please ensure reference bandwidth is consistent across all routers
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.12 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to configure link detection through bidirectional forwarding detection (BFD) for all the interfaces running OSPF.

Run the **no** form of this command to restore the default configuration.

By default, the BFD function is disabled on all the interfaces.

Syntax

bfd all-interfaces

no bfd all-interfaces

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPF protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, OSPF establishes a BFD session with a neighbor in the full neighbor relationship to detect the neighbor status through the BFD mechanism. When the BFD neighbor fails, OSFP immediately performs network convergence.

You can also configure the **ip ospf bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the **bfd all-interfaces** command used in OSPF process configuration mode.

Examples

The following example configures all interfaces running OSPF to conduct BFD link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# bfd all-interfaces
```

Notifications

When the neighbor device also needs to be configured with BFD to prevent route learning from being affected, the following notification will be displayed:

```
% Warning: The BFD for OSPF neighbor shall be enabled, or it would affect the route
learning.
```

Common Errors

BFD is not enabled on the interconnected devices at the same time.

Platform Description

N/A

Related Commands

- **show ip ospf**

1.13 capability opaque

Function

Run the **capability opaque** command to enable the opaque LSA processing capability.

Run the **no** form of this command to disable the opaque LSA processing capability.

The opaque LSA processing capability is enabled by default.

Syntax

capability opaque

no capability opaque

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the opaque LSA processing capability.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# no capability opaque
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.14 capability vrf-lite

Function

Run the **capability vrf-lite** command to forcibly disable the automatic judging function of support to loop detection for OSPF processes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the automatic judging function of support to loop detection is enabled for the OSPF processes associated with VRF.

Syntax

capability vrf-lite [**auto**]

no capability vrf-lite [**auto**]

default capability vrf-lite [**auto**]

Parameter Description

auto: Automatically judges whether loop detection is supported for the OSPF processes associated with VRF.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only for the OSPF process associated with VRF.

By default, support to loop detection and PE-CE OSPF feature is automatically judged for the OSPF processes associated with VRF.

- The **capability vrf-lite** command can be used to forcedly disable the above function.
- The **no capability vrf-lite** command can be used to forcedly enable the above function.
- The **capability vrf-lite auto** command is configured to enable the OSPF process associated with VRF to automatically judge whether the above function is enabled.
- The **capability vrf-lite auto** command is used to restore the default configuration.

Loop detection of OSPF processes aims to prevent possible loop of VPN routes in propagation. When an OSPF process associated with VRF receives LSA, it will process the LSA according to the following principle:

- After the loop detection function is disabled, the OSPF protocol will not check the DN bit (down bit) and VPN route tag in the LSA packet after receiving the LSA packet, and allow the LSA to participate in the calculation of OSPF.
- For type-3, 5 and 7 LSAs, the DN bit is detected. If the received LSA contains a DN bit, the LSA does not participate in OSPF calculation.
- For type-5 and 7 LSAs, the VPN route tag (Domain-tag) is detected. If the VPN route tag of the received LSA is the same as that of the local OSPF process, the LSA does not participate in the OSPF calculation.

The so-called PE-CE OSPF feature converts different OSPF LSAs for advertising to CE according to the BGP extended attribute of route. After the OSPF feature of PE-CE is disabled, different OSPF LSAs are not converted according to BGP attributes.

By default, support to loop detection is automatically judged for the OSPF processes associated with VRF. The purpose of this function is as follows:

In some application scenarios, you may need to disable the loop detection function of VRF OSPF processes. For example, VPN users use MCE devices to exchange VPN routes with PEs. If the OSPF protocol runs between MCEs and PEs to exchange VPN routes, to enable the MCE to learn the VPN route advertised by the PE and advertise it to the downlink VPN site, you need to disable the loop detection function of VRF OSPF processes of the MCE device. For the general MCE scenario, currently the device can automatically judge and disable the loop detection feature of OSPF processes. If the automatic judgment result is incorrect, you need to run the [**no**] **capability vrf-lite** command to forcibly enable or disable the loop detection feature of OSPF processes.

Examples

The following example disables the loop detection capability for OSPF processes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# capability vrf-lite
```

Notifications

If the OSPF process is not bound to VRF, the following notification will be displayed:

```
% The command CAN NOT apply to ospf instance bound to VRF default.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 clear ip ospf process

Function

Run the **clear ip ospf process** command to clear and restart an OSPF process.

Syntax

clear ip ospf [*process-id*] **process**

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535. When this parameter is specified, the specified OSPF process will be cleared and reset. When this parameter is not specified, all the running OSPF processes will be cleared and reset.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Resetting the whole OSPF process will reestablish all the neighbors, which has a great impact on the entire protocol.

When running this command, you need to make confirmation.

Examples

The following example clears and resets OSPF Process 1.

```
Hostname> enable
Hostname# clear ip ospf 1 process
Reset OSPF process! [yes/no]:
```

Notifications

When an OSPF process not existing is reset, the following notification will be displayed:

```
%OSPF: No router process 1
```

Platform Description

N/A

1.16 compatible rfc1583

Function

Run the **compatible rfc1583** command to enable the RFC1583 rules.

Run the **no** form of this command to disable the RFC1583 rules.

The RFC1583 rules are enabled by default.

Syntax

compatible rfc1583

no compatible rfc1583

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When multiple paths reach the same external destination of AS, the optimum path must be determined. This command determines to run the priority rule used in the RFC1583 rules.

Examples

The following example configures the RFC1583 rules to determine the optimum route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# no compatible rfc1583
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.17 default-information originate

Function

Run the **default-information originate** command to generate a default route to be injected to the OSPF routing domain.

Run the **no** form of this command to disable the default route.

No default route is generated by default.

Syntax

default-information originate [**always** | **metric** *metric* | **metric-type** *type* | **route-map** *map-name*] *

no default-information originate [**always** | **metric** | **metric-type** | **route-map**] *

Parameter Description

always: Enables OSPF to generate a default route no matter whether the local router has a default route.

metric *metric*: Indicates the initial metric of the default route. The value range is from 0 to 16777214, and the default value is **1**.

metric-type *type*: Indicates the type of the default route. The default value is 2. OSPF external routes are classified into two types. Type 1: The metric varies with routers. Type 2: The metric is the same for all the routers. Type 1 external routes are more trustworthy than Type 2 external routes.

route-map *map-name*: Indicates the name of the associated route map. No route map is associated by default.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

After the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To enable the ASBR to generate a default route, configure the **default-information originate** command.

If the **always** parameter is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether a default route is generated, run the **show ip ospf database** command to display the OSPF link state database (LSDB). The external link with ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route.

The metric of the external default route can be set only by running the **default-information originate** command, instead of the **default-metric** command.

OSPF has two types of external routes. The metric of the Type-1 external route changes, but the metric of the Type-2 external route is fixed. If two parallel paths to the same destination have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ip route** command displays only the Type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA. If you want to generate a default route in the NSSA, run the **area nssa default-information-originate** command.

A router in the stub area cannot generate an external default route.

The metric value range configured for the associated route map is 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

Examples

The following example configures an external default route for the OSPF routing domain with type set to **1** and metric set to **50**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.24.0 0.0.0.255 area 0
Hostname(config-router)# default-information originate always metric 50 metric-type
1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf database**
- **show ip route** (route management)

1.18 default-metric

Function

Run the **default-metric** command to configure the default metric for an OSPF redistributed route.

Run the **no** form of this command to restore the default configuration.

By default, the metric of a redistributed route is 20.

Syntax

default-metric *metric*

no default-metric

Parameter Description

metric: Default metric of the OSPF redistributed route. The value range is from 1 to 16777214.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The **default-metric** command must be used together with the **redistribute** command to modify the initial metrics of all redistributed routes.

Setting the **default-metric** command does not take effect on the external routes that are configured and injected to the OSPF routing domain using the **default-information originate** command.

Examples

The following example sets the default metric value of an OSPF redistributed route to **50**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# version 2
Hostname(config-router)# exit
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.10.0 0.0.0.255 area 0
Hostname(config-router)# default-metric 50
Hostname(config-router)# redistribute rip subnets
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **redistribute**
- **show ip ospf database**

1.19 disable-dn-bit-check

Function

Run the **disable-dn-bit-check** command to disable the DN bit loop detection function of LSA.

Run the **no** form of this command to enable the function.

Run the **default** form of this command to restore the default configuration.

The DN bit loop detection function of LSA is enabled by default.

Syntax

disable-dn-bit-check [**summary** | **ase** | **nssa**]

no disable-dn-bit-check [**summary** | **ase** | **nssa**]

default disable-dn-bit-check [**summary** | **ase** | **nssa**]

Parameter Description

summary: Disables DN bit check of the summary LSA.

ase: Disables DN bit check of the AS-External LSA.

nssa: Disables DN bit check of the NSSA LSA.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In the CE dual-homing scenario of L3VPN, loop is avoided by suppressing the route computation of DN bit between PEs. However, in a specific scenario, PEs may be allowed to learn routes from each other without generating any loops. In this case, check of the DN bit can be cancelled using this command.

When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the DN bit will not be checked.

Type-3, Type-5, and Type-7 LSAs of OSPF can all carry a DN bit.

Examples

The following example disables loop detection using the DN bit of summary LSA under the VRF OSPF process VPN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# disable-dn-bit-check summary
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 disable-tag-check

Function

Run the **disable-tag-check** command to disable loop detection using the route tag of LSA.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The loop detection function using the route tag of LSA is enabled by default.

Syntax

disable-tag-check

no disable-tag-check

default disable-tag-check

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In the CE dual-homing scenario of L3VPN, when the LSA route tag received by a PE is the same as its route tag, the route is not calculated, thus avoiding loop.

In a specific scenario, PEs are allowed to learn routes from each other without generating any loops. In this case, you can configure different route tags for multiple PEs, or configure to disable route tag check.

When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the route tag will not be checked.

Type-5 and Type-7 LSAs of OSPF can carry a route tag.

Examples

The following example disables loop detection using the route tag of LSA under the VRF OSPF process VPN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# disable-tag-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 discard-route

Function

Run the **discard-route** command to allow adding a discard route to the core routing table.

Run the **no** form of this command to remove this configuration.

The discard route adding function is enabled by default.

Syntax

discard-route { **internal** | **external** }

no discard-route { **internal** | **external** }

Parameter Description

internal: Allows adding the inter-area route summarization command, namely, the discard route generated by the **area range** command.

external: Allows adding the external route summarization command, namely, the discard route generated by the **summary-address** command.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

During route summarization, the range after summarization may exceed the actual network scope in the routing table. If the data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table on the ABR or ASBR. This route is automatically generated, and is not advertised.

Examples

The following example prohibits adding a discard route to the core routing table.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# no discard-route internal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (route management)

1.22 distance

Function

Run the **distance** command to configure the management distances corresponding to different types of OSPF routes.

Run the **no** form of this command to restore the default configuration.

By default, the management distance is **110** for all the OSPF routes.

Syntax

distance { *distance* [**route-map** *map-name*] | **ospf** { [**intra-area** *distance* [**route-map** *map-name*]] [**inter-area** *distance* [**route-map** *map-name*]] [**external** *distance* [**route-map** *map-name*]] } }

no distance [**ospf**]

Parameter Description

distance: Management distance of a route. The value range is from 1 to 255.

intra-area *distance*: Indicates the management distance of an intra-area route. The value range is from 1 to 255.

inter-area *distance*: Indicates the management distance of an inter-area route. The value range is from 1 to 255.

external *distance*: Indicates the management distance of an external route. The value range is from 1 to 255.

route-map *map-name*: Indicates the name of the associated route map. No route map is associated by default.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To compare the priorities of routes generated by different OSPF processes, you need to run this command to specify the management distances corresponding to different types of OSPF routes.

The management distance allows different routing protocols to compare route priorities. A smaller management distance indicates a higher route priority.

If the management distance of a route entry is set to 255, the route entry is not trustworthy and does not participate in packet forwarding.

Configure the **route-map** parameter and set a management distance for the specific route through a policy. If **route-map** is configured with **set distance**, then:

- For a matched route, the management distance is set by the **set distance** command.
- For an unmatched route, the management distance is set by the **distance** command.

Examples

The following example sets the management distance of an OSPF external route to **160**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# distance ospf external 160
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (route management)

1.23 distribute-list in

Function

Run the **distribute-list in** command to configure filtering routes that are calculated based on the received LSA.

Run the **no** form of this command to remove this configuration.

By default, the filtering function of the routes calculated based on the received LSA is disabled, that is, all these routes get past.

Syntax

istribute-list { *acl-name* | *acl-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

no distribute-list { *acl-name* | *acl-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL No. The following value ranges are supported. The value range of IP standard ACL is 1 to 99 or 1300 to 1999; the value range of IP extended ACL is 100 to 199 or 2000 to 2699.

gateway *prefix-list-name*: Uses the gateway for filtering.

prefix *prefix-list-name*: Uses a prefix list for filtering.

route-map *route-map-name*: Uses a route map for filtering.

interface-type interface-number: interface for which LSA routes are filtered.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This function filters the routes that are computed based on received LSAs. Only the routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL, prefix list, and route map filtering rules are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes of a specified interface, prefix list or router map cannot be configured for filtering routes of the same interface.

The route map used in this command supports the following **match** commands:

- **match interface**
- **match ip address**
- **match ip address prefix-list**
- **match ip next-hop**
- **match ip next-hop prefix-list**
- **match metric**
- **match route-type**
- **match tag**

Caution

Filtering routes by running the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type-3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black hole routes.

Examples

The following example configures ACL 3 to filter the routes received by GigabitEthernet 0/1 and calculated based on the received LSA.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 3 permit 172.16.0.0 0.0.127.255
Hostname(config)# router ospf 25
Hostname(config-router)# distribute-list 3 in GigabitEthernet 0/1
```

Notifications

When an invalid interface is configured, the following notification will be displayed:

```
% Interface is invalid.
```

When an invalid ACL name is configured, the following notification will be displayed:

```
% ACL name abc-acl is invalid
```

When routes imported by this instance are filtered, the following notification will be displayed:

```
% Distribute-list of "ospf 1" via "ospf 1" not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (route management)

1.24 distribute-list out

Function

Run the **distribute-list out** command to configure filtering of redistributed routes.

Run the **no** form of this command to disable filtering of redistributed routes.

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes get past.

Syntax

distribute-list { *acl-number* | *acl-name* | **prefix** *prefix-list-name* } **out** [**arp-host** | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *acl-number* | *acl-name* | **prefix** *prefix-list-name* } **out** [**arp-host** | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

acl-number: ACL No. The following value ranges are supported. The value range of IP standard ACL is 1 to 99 or 1300 to 1999; the value range of IP extended ACL is 100 to 199 or 2000 to 2699.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

prefix *prefix-list-name*: Uses a prefix list for filtering.

arp-host: Filters host routes converted by Address Resolution Protocol (ARP).

bgp: Filters BGP routes.

connected: Filters direct routes.

isis [*area-tag*]: Filters IS-IS routes.

ospf *process-id*: Filters OSPF routes.

rip: Filters RIP routes.

static: Filters static routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The **distribute-list out** command is similar to the **redistribute route-map** command, and is used to filter routes that are redistributed from other protocols to OSPF. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and prefix list filtering rules are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes coming from a certain source, the prefix list cannot be configured to filter the same routes.

Examples

The following example filters the redistributed static routes according to the prefix list jjj.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# redistribute static subnets
Hostname(config-router)# distribute-list prefix jjj out static
```

Notifications

When the **gateway** parameter is carried for filtering of redistributed routes, the following notification will be displayed:

```
% Gateway not allowed with OUT in distribute-list cmd
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf database**

1.25 domain-id

Function

Run the **domain-id** command to configure the domain ID of an OSPF process.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the domain ID value of an OSPF process is **null**, and the type value is **0005**.

Syntax

domain-id { *ipv4-address* [**secondary**] | **null** | **type** { **0005** | **0105** | **0205** | **8005** } **value** *hex-value* [**secondary**] }

no domain-id [*ipv4-address* [**secondary**] | **null** | **type** { **0005** | **0105** | **0205** | **8005** } **value** *hex-value* [**secondary**]]

default domain-id

Parameter Description

ipv4-address: IPv4 address as the domain ID.

secondary: Uses the configured domain ID as a secondary identifier.

null: Indicates that the OSPF process has no domain ID.

type { **0005** | **0105** | **0205** | **8005** }: Sets the domain ID type of an OSPF process. Its value can be one of the following four types: 0x0005, 0x0105, 0x0205, and 0x8005. The default value is 0x0005.

value *hex-value*: Sets the domain ID value of an OSPF process, a hexadecimal value indicating a 6-byte number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only on the OSPF process associated with VRF.

If an OSPF process is configured with a domain ID, when an OSPF route is redistributed to BGP and becomes a VPN route, the domain ID will be redistributed to BGP together, and finally will be advertised to other PEs as one part of the extcommunity attribute in the VPN route.

You can run the **domain-id secondary** command to configure multiple domain IDs of an OSPF process. However, there can be only one primary domain ID, and the remaining ones are secondary domain IDs. When the OSPF route is converted to a VPN route for advertising, the corresponding extcommunity attribute will carry the primary domain ID information only.

In general, the OSPF protocol runs between the PE and CE for VPN route interaction. After the PE receives a VPN route and redistributes it to the OSPF process, the route will be advertised to the VPN site as a Type-5 LSA. However, for different sites belonging to the same OSPF domain, the route should be advertised as a Type-3 LSA. Therefore, the same domain ID can be configured for the corresponding VRF OSPF process on the PE so as to advertise the route within the domain as a Type-3 LSA.

The domain IDs of different VRF OSPF processes on the same PE do not influence each other, and can be configured the same or different. However, the VRF OSPF processes that belong to the same VPN must be configured with the same domain ID to ensure the correctness of route advertising.

Examples

The following example configures the domain ID type under VRF OSPF process VPN 1 as 0005 and the domain ID value as 000000000001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# domain-id type 0005 value 000000000001
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.26 domain-tag

Function

Run the **domain-tag** command to configure the VPN route tag of an OSPF process associated with VRF.

Run the **no** form of this command to restore the default value.

Run the **default** form of this command to restore the default configuration.

By default, the default value of a VRF OSPF process is the AS number of the local BGP protocol.

Syntax

domain-tag *tag*

no domain-tag

default domain-tag

Parameter Description

tag: VPN route tag value of an OSPF process. The value range is from 1 to 4294967295.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only for the OSPF process associated with VRF and BGP redistributed routes.

If a VPN site is connected to multiple PEs, the VPN route will be learned from the PE through MP-BGP. If the route is advertised to the VPN site through a Type- 5 or Type-7 LSA, it may be learned and advertised by other PEs connected to the VPN site, which may cause a loop. To prevent loops, the VRF OSPF processes connected to the same VPN site on the PEs are configured with the same VPN route tag. When a VRF OSPF process sends a Type-5 or Type-7 LSA to a VPN site, the VPN route tag information will also be attached to the LSA. When other PE sites receive such a Type-5 or Type-7 LSA, if they detect that the VPN route tag in the LSA is consistent with that of the local OSPF process, the LSA will not participate in the OSPF computation.

Generally, the OSPF processes belonging to the same VPN site are configured with the same VPN route tag value.

The VPN route tag occupies four bytes in an OSPF packet. If a VRF OSPF process is not configured with this command, when the OSPF process advertises a Type-5 or Type-7 LSA, the first two bytes of the VPN route tag

are set to 0xD000 by default, and the last two bytes are the AS number of the local BGP. For example, if the AS number of the local BGP is 1, the hexadecimal form of the VPN route tag is: 0xD0000001.

Examples

The following example configures the route tag of the OSPF process VPN1 associated with VRF as **10**.

```
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# domain-tag 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 enable mib-binding

Function

Run the **enable mib-binding** command to bind the MIB to a specified OSPFv2 process.

Run the **no** form of this command to restore the default binding.

By default, the MIB is bound to the OSPFv2 process with the minimum process ID.

Syntax

enable mib-binding

no enable mib-binding

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP.

If you wish to perform operations on a specified OSPFv2 through SNMP, run this command to bind the MIB with the process.

Examples

The following example configures to bind the MIB to the specified OSPFv2 process 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 100
Hostname(config-router)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 enable traps

Function

Run the **enable traps** command to enable sending of the specified trap message.

Run the **no** form of this command to disable sending of the specified trap message.

The trap message sending function is disabled by default.

Syntax

enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange** | **VirtNbrStateChange**]]

no enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange** | **VirtNbrStateChange**]]

Parameter Description

error: Configures all the trap switches related to Error. This parameter can also configure the following specific error trap switches:

IfAuthFailure: Indicates interface authentication error.

IfConfigError: Indicates interface parameter configuration error.

IfRxBadPacket: Indicates that the interface receives an error packet.

VirtIfAuthFailure: Indicates virtual interface authentication error.

VirtIfConfigError: Indicates virtual interface parameter configuration error.

VirtIfRxBadPacket: Indicates that the virtual interface receives an error packet.

lsa: Configures all the trap switches related to LSA. This parameter can also configure the following specific LSA trap switches:

LsdbApproachOverflow: Indicates that the number of external LSAs has reached 90% of the upper limit.

LsdbOverflow: Indicates that the number of external LSAs has reached the upper limit.

MaxAgeLsa: Indicates that the LSA aging timer expires.

OriginateLsa: Indicates that a new LSA is generated.

retransmit: Configures all the trap switches related to Retransmit. This parameter can also configure the following specific retransmit trap switches:

IfTxRetransmit: Indicates that a packet is retransmitted on the interface.

VirtIfTxRetransmit: Indicates that a packet is retransmitted on the virtual interface.

state-change: Configures all the trap switches related to State-change. This parameter can also configure the following specific state-change trap switches:

IfStateChange: Indicates that the interface state changes.

NbrRestartHelperStatusChange: Indicates that the status of the neighbor GR process changes.

NbrStateChange: Indicates that the neighbor state changes.

NssaTranslatorStatusChange: Indicates that the NSSA translator state changes.

RestartStatusChange: Indicates that the GR status of the local device changes.

VirtIfStateChange: Indicates that the virtual interface state changes.

VirtNbrRestartHelperStatusChange: Indicates that the status of the virtual neighbor GR process changes.

VirtNbrStateChange: Indicates that the virtual neighbor state changes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Currently the OSPFv2 process supports sending of 16 kinds of trap messages, which are classified into four types.

The function configured by this command is restricted by the **snmp-server** command. You can must configure the **snmp-server enable traps ospf** command and then the **enable traps** command before the corresponding OSPF trap message can be correctly sent out.

This command is not restricted by the MIB bound to the process. The trap switch can be enabled concurrently for different processes.

Examples

The following example enables sending of the specified trap message.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 100
Hostname(config-router)# enable traps
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **snmp-server enable traps ospf** (network management and monitoring/SNMP)

1.29 extcommunity-type

Function

Run the **extcommunity-type** command to configure the Router-ID or Route-Type of an OSPF process associated with VRF.

Run the **no** form of this command to restore the default type value.

Run the **defaulttype** form of this command to restore the default configuration.

By default, the type of Router-ID is 0107, and the type of Route-Type is 0306.

Syntax

extcommunity-type { **router-id** { **0107** | **8001** } | **route-type** { **0306** | **8000** } } *

no extcommunity-type { **router-id** | **route-type** } *

default extcommunity-type { **router-id** | **route-type** } *

Parameter Description

router-id { **0107** | **8001** }: Sets the Router-ID of an OSPF process. Its value is **0107** or **8001**.

route-type { **0306** | **8000** }: Sets the Router-Type of an OSPF process. Its value is **0306** or **8000**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only for the OSPF process associated with VRF, but is invalid for the global VRF instance configuration.

When an OSPF route of VRF forms a VPN route, the Router-ID information of the OSPF process will also be carried in the extcommunity attribute of the VPN route. You can run the **extcommunity-type router-id** command to specify the value of the type field in the extcommunity attribute as **0x0107** or **0x8001**.

When an OSPF route of VRF forms a VPN route, the Route-Type information of the OSPF process will also be carried in the extcommunity attribute of the VPN route. You can run the **extcommunity-type roue-type** command to specify the value of the type field in the extcommunity attribute as **0x0306** or **0x8000**.

Examples

The following example configures the Router-ID of the OSPF process VPN1 associated with VRF as **8001**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# extcommunity-type router-id 8001
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 fast-reroute

Function

Run the **fast-reroute** command to configure the OSPF fast reroute function of a device.

Run the **no** form of this command to restore the default configuration.

The fast reroute function is disabled by default.

Syntax

fast-reroute { **lfa** [**downstream-paths**] | **route-map** *route-map-name* }

no fast-reroute { **lfa** [**downstream-paths**] | **route-map**] }

Parameter Description

lfa: Enables computation of the loop-free backup path.

downstream-paths: Enables computation of the downstream path.

route-map *route-map-name*: Specifies a backup path through the route map.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If the **lfa** parameter is configured, computation of the loop-free backup path is enabled. Now, you can run the interface mode command to specify the path protection mode of the interface.

It is recommended that automatic computation of LFA for the backup path be disabled if any of the following cases exists on the network:

- Virtual links exist.
- Alternative ABRs exist.
- An ASBR is also an ABR.
- Multiple ABSRs advertise the same external route.

If both **lfa** and **downstream-paths** are configured, computation of the downstream path is enabled.

If **route-map** is configured, a backup path can be specified for a matched route through the route map.

When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time, so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is up or down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure **carrier-delay 0** on a Layer-3 interface to achieve the fastest switchover speed.

Note

- Currently, the OSPF fast reroute function is subject to the following constraints:
- Only one backup next hop can be generated for one route.
- No backup next hop can be generated for equal-cost multi-path routing (ECMP).

Examples

The following example configures the FRR function of OSPF process 1 and associates it with fast-reroute of the route map.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map fast-reroute
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1
backup-nexthop 192.168.1.2
Hostname(config)# router ospf 1
Hostname(config-router)# fast-reroute route-map fast-reroute
```

Notifications

When the route map name exceeds 32 characters, the following notification will be displayed:

```
% Route-map name string length can not exceed 32
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **carrier-delay** (interface/Ethernet interface)
- **show ip route** (route management)

1.31 graceful-restart

Function

Run the **graceful-restart** command to enable the OSPF GR capability and set the GR period.

Run the **no** form of this command to disable the OSPF GR capability or restore the default value of the GR period.

The OSPF GR capability is enabled by default.

Syntax

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*grace-period*]

Parameter Description

grace-period *grace-period*: Sets the GR period, in seconds, which is the maximum time from occurrence of an OSPF failure to restart of OSPF and completion of the OSPF GR. The value range is 1 to 1800, and the default value is **120**.

inconsistent-lsa-checking: Enables topology change detection. If any topology change is detected, OSPF exits the GR process to complete convergence.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When a GR-enabled device is restarted on the control plane, data forwarding can be guided on the forwarding plane. In addition, actions such as neighbor relationship re-forming and route computation performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions.

This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link state is rebuilt so that the original state of the OSPF process is restored. After the GR period expires, OSPF exits the GR state and performs common OSPF operations.

Run the **graceful-restart** command to set the GR period to 120s. The **graceful-restart grace-period** command allows you to modify the GR period explicitly.

If the Fast Hello function is enabled, the GR function cannot be enabled.

The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole.

- Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time.
- Configuring topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled.

In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process.

Examples

The following example enables the OSPF restarter capability and sets the GR period to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# graceful-restart grace-period 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.32 graceful-restart helper

Function

Run the **graceful-restart helper** command to enable the OSPF GR helper function and configure the relevant topology change detection mode.

Run the **no** form of this command to remove this configuration.

The GR helper capability is enabled by default. After the GR helper is enabled on the device, LSA changes are not checked.

Syntax

graceful-restart helper { **disable** | **strict-lsa-checking** | **internal-lsa-checking** }

no graceful-restart helper { **disable** | **strict-lsa-checking** | **internal-lsa-checking** }

Parameter Description

disable: Prohibits a device from acting as a GR helper for another device.

strict-lsa-checking: Indicates that changes in Type-1 to Type-5 and Type-7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

internal-lsa-checking: Indicates that changes in Type-1 to Type-3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the GR helper capability of a device. When a neighbor device implements GR, it sends a Grace-LSA to notify all neighbor devices. If the GR helper function is configured on the local device, the local device becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that the GR helper is not provided for any device that implements GR.

After a device becomes a GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or configure **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (strict-lsa-checking and internal-lsa-checking) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Examples

The following example disables the OSPF GR helper function and configures the relevant topology change detection mode as **strict-lsa-checking**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# graceful-restart helper disable
Hostname(config-router)# no graceful-restart helper disable
Hostname(config-router)# graceful-restart Helper strict-lsa-checking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.33 ip ospf authentication

Function

Run the **ip ospf authentication** command to configure the authentication mode of an interface.

Run the **no** form of this command to restore the default authentication mode.

By default, no authentication mode is set on an interface. In this case, the authentication type of the related area is used on the interface.

Syntax

ip ospf authentication [**message-digest** | **null** | **keychain** *kc-name*]

no ip ospf authentication

Parameter Description

message-digest: Indicates that MD5 encryption authentication is enabled on the current interface.

null: Indicates that authentication is disabled.

keychain *kc-name*: Indicates that keychain authentication is configured. If **Keychain** specifies that the authentication type is **SM3**, the key ID value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **ip ospf authentication** command does not contain any option, plain text authentication is enabled. If you run the **no** form of this command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to **null**, authentication is disabled forcibly. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, MD5 authentication, and SM3 authentication.

Examples

The following example configures the OSPF authentication type of GigabitEthernet 0/1 interface as MD5 authentication.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf authentication message-digest
```

The following example configures the OSPF authentication type of the GigabitEthernet 0/1 interface as keychain authentication and the key chain as hello.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf authentication keychain ospf
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# key chain ospf
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string hello
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 ip ospf authentication-key

Function

Run the **ip ospf authentication-key** command to configure the plain text authentication key of OSPF.

Run the **no** form of this command to delete the plain text authentication key.

The authentication key is disabled by default.

Syntax

ip ospf authentication-key [**0** | **7**] *key*

no ip ospf authentication-key

Parameter Description

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: The key, a string of up to eight characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The key configured by the **ip ospf authentication-key** command is inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF neighbor relationship and therefore cannot exchange the routing information.

Different keys can be configured for different interfaces, but all routers connected to the same physical network segment must be configured with the same key.

You can enable or disable authentication in an OSPF area by running the **area authentication** command.

You can enable authentication on an individual interface by running **ip ospf authentication** in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

Examples

The following example configures the OSPF authentication mode of the GigabitEthernet 0/1 interface as **ospfauth**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf authentication-key ospfauth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **area authentication**
- **ip ospf authentication**

1.35 ip ospf area

Function

Run the **ip ospf area** command to configure an OSPF routing process in which an interface participates.

Run the **no** form of this command to prevent an interface from participating in the OSPF routing process.

The OSPF routing process is disabled on an interface by default.

Syntax

ip ospf *process-id* **area** *area-id*

no ip ospf *process-id* **area** *area-id*

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area-id: ID of the OSPF area in which the interface participates, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Running this command will add all IP addresses on the interface to the OSPF process.

You can also add an interface to OSPF process using the **network** command on the instance. If two commands are run at the same time, the configuration on the interface takes effect first.

Examples

The following example enables the GigabitEthernet 0/1 interface to participate in Area 0 of OSPF Routing Process 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf 1 area 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.36 ip ospf bfd

Function

Run the **ip ospf bfd** command to configure an OSPF-enabled interface to enable or disable the BFD function.

Run the **no** form of this command to configure an OSPF-enabled interface to disable the BFD function.

The BFD function is disabled on an interface by default.

Syntax

ip ospf bfd [**disable**]

no ip ospf bfd

Parameter Description

disable: Disables BFD link detection on the OSPF-enabled interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Once a link is faulty, OSPF can quickly detect the failure of the route. Configuring this command helps shorten the traffic interruption time.

The **ip ospf bfd** command configured on an interface takes precedence over the **bfd all-interfaces** command used in process configuration mode.

In light of the actual environment, you can run the **ip ospf bfd** command to configure BFD link detection on the specified interface, or run the **bfd all-interfaces** command in OSPF process configuration mode to configure BFD for link detection on all the interfaces of the OSPF process. You can run the **ip ospf bfd disable** command to disable BFD for link detection on the specified interface.

Examples

The following example configures the OSPF-enabled GigabitEthernet 0/1 interface to conduct BFD link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.37 ip ospf cost

Function

Run the **ip ospf cost** command to configure the cost value for an OSPF interface to send a packet.

Run the **no** form of this command to restore the default value.

By default, the cost value of an OSPF interface is automatically calculated.

Syntax

ip ospf cost *cost*

no ip ospf cost

Parameter Description

cost: Cost value of an OSPF interface. The value range is from 0 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By default, the cost of an OSPF interface is equal to the reference value of the interface bandwidth divided by the actual interface bandwidth.

You can run the **auto-cost** command to configure the bandwidth reference value of an interface. The default value is 100 Mbps.

Run the **bandwidth** command to set the interface bandwidth.

The default costs of OSPF interfaces on several typical lines are as follows:

- For the 64 Kbps serial line, the cost is 1562.
- For the E1 line, the cost is 48.
- For the 10 Mbps Ethernet, the cost is 10.
- For the 100 Mbps Ethernet, the cost is 1.

Configuring the cost value of an OSPF interface through the **ip ospf cost** command will overwrite the default configuration.

Examples

The following command configures the cost for the OSPF-enabled GigabitEthernet 0/1 interface to send a packet as **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf cost 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.38 ip ospf cost-fallback

Function

Run the **ip ospf cost-fallback** command to configure the cost fallback of an aggregation port (AP).

Run the **no** form of this command to disable the cost fallback of an AP.

The cost fallback function is disabled on an AP by default.

Syntax

ip ospf cost-fallback *cost* **threshold** *bandwith*

no ip ospf cost-fallback

Parameter Description

cost: Cost fallback value. The value range is from 1 to 65535.

threshold *bandwith*: Indicates the bandwidth threshold, in bytes per second. When the AP bandwidth is smaller than this value, the cost fallback value takes effect. The value range is from 1 to 4294967.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The bandwidth of an AP is equal to the sum of the bandwidths of all the valid member ports. When a member port fails, the bandwidth of the AP will be reduced. You can set a cost fallback value for the AP to enable OSPF to select other paths preferably. When the failed member port recovers, the cost fallback value becomes invalid, and the metric of the AP returns to normal.

Examples

The following example configures the cost fallback value for an AP, and sets the metric to 100 when the bandwidth is smaller than 1,000 Mbps.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface AggregatePort 1
Hostname(config-if-AggregatePort 1)# ip ospf cost-fallback 100 threshold 1000
```

Notifications

When a cost fallback value is configured for a non-AP, the following notification will be displayed:

```
%OSPF: Warning: Only aggregate ports are suitable for this command
```

Common Errors

Cost fallback is enabled on a non-AP.

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.39 ip ospf database-filter all out

Function

Run the **ip ospf database-filter all out** command to prevent an interface from diffusing LSA packets to the outside, that is, LSA update packets are not sent from the interface.

Run the **no** form of this command to restore the default value.

By default, the function of not diffusing LSA packets to the outside is disabled on an interface, that is, any LSA update packet can be sent from the interface.

Syntax

ip ospf database-filter all out

no ip ospf database-filter

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To prevent an interface from sending LSA update packets, you can enable this function on the interface. After this function is enabled, the local device does not advertise the LSA update packet to neighbors, but still sets up a neighbor relationship with neighbors and receives LSAs from neighbors.

Examples

The following example prevents the GigabitEthernet 0/1 interface from diffusing LSA packets to the outside.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf database-filter all out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.40 ip ospf dead-interval

Function

Run the **ip ospf dead-interval** command to configure the interval for OSPF to determine the failure of a specified interface neighbor.

Run the **no** form of this command to restore the default configuration.

By default, the fast hello function is disabled, and the neighbor dead interval is four times the sending interval of hello packet.

Syntax

ip ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* }

no ip ospf dead-interval

Parameter Description

Dead-interval: Interval for determining failure of a neighbor, in seconds. The value range is from 0 to 2147483647.

minimal: Enables the fast hello function and sets the interval for determining failure of a neighbor to 1s.

hello-multiplier *multiplier*: Specifies the number of hello packets sent per second in the fast hello function. The value range is from 3 to 20.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The failure determining interval of an OSPF neighbor is contained in the hello packet. If OSPF does not receive a hello packet from a neighbor within the neighbor dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. The neighbor dead interval is four times the sending interval of hello packet. If the hello interval is modified, the neighbor dead interval is modified automatically.

You can run this command to manually modify the interval for OSPF to judge failure of a neighbor. However, note the following points:

(1) The neighbor dead interval cannot be smaller than the hello packet sending interval.

(2) The neighbor dead interval must be the same on all routers in the same network segment.

After the OSPF fast hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF fast hello function by specifying the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter. The **minimal** keyword indicates that the neighbor dead interval is set to 1s, and **hello-multiplier** indicates the number of hello packets sent per second. In this way, the interval at which the hello packet is sent decreases to less than 1s.

If the fast hello function is configured for an interface, the hello interval field of the hello packet advertised on the interface is set to 0, and the hello interval field of the hello packet received on this interface is ignored.

No matter whether the fast hello function is enabled, the neighbor dead interval must be always consistent in the same network segment. The **hello-multiplier** value can be inconsistent provided that at least one hello packet can be received within the neighbor dead interval. The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the fast hello function cannot be configured simultaneously.

Run the **show ip ospf interface** command to monitor the neighbor dead interval and the fast hello interval configured for an interface.

Examples

The following example configures the interval for OSPF to judge failure of a neighbor on the GigabitEthernet 0/1 interface as **30**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 30
```

The following example enables the fast hello function of the GigabitEthernet 0/1 interface and configures Hello-multiplier as **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf dead-interval minimal
hello-multiplier 3
```

Notifications

N/A

Common Errors

The neighbor dead intervals configured on different devices in the same area are inconsistent.

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.41 ip ospf disable all

Function

Run the **ip ospf disable all** command to prevent a specified interface from generating OSPF packets.

Run the **no** form of this command to restore the default state.

By default, an interface is allowed to generate OSPF packets.

Syntax

ip ospf disable all

no ip ospf disable all

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The interface configured with this command ignores whether **network area** is matched. After this command is configured, even if the interface belongs to the network segment range advertised by the **network** command, it will not generate OSPF packets any more. Therefore, the interface will neither send/receive any OSPF packet, nor participate in OSPF computation.

Examples

The following example prevents the GigabitEthernet 0/1 interface from generating LSA packets any more.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf disable all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.42 ip ospf fast-reroute protection

Function

Run the **ip ospf fast-reroute protection** command to enable the loop-free alternate (LFA) protection mode of a specified interface.

Run the **no** form of this command to restore the default configuration.

The LFA link protection function is enabled by default.

Syntax

ip ospf fast-reroute protection { **node** | **link-node** | **disable** }

no ip ospf fast-reroute protection

Parameter Description

node: Enables the LFA node protection.

link-node: Enables the LFA link node protection.

disable: Disables LFA protection.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After you run the **fast-reroute lfa** command in OSPF routing process configuration mode, OSPF fast reroute calculation will be enabled, and a standby route will be generated for the primary route based on the LFA protection mode specified in interface configuration mode. By default, LFA protection is enabled on each OSPF interface, and the failure of the active link does not affect data forwarding on the standby route.

- Run the **node** parameter to enable node protection for the interface, that is, data forwarding on the standby route will not be affected by the failure of a neighbor node corresponding to the active link.
- Run the **link-node** parameter to protect both the link and neighbor node corresponding to the primary route.
- Run the **disable** parameter to disable the LFA protection function of the interface, that is, no backup entry will be generated for the route whose next hop is the interface.

This command does not take effect if **fast-rerotue route-map** is configured.

Examples

The following example enables LFA link node protection on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf fast-reroute protection link-node
```

Notifications

N/A

Common Errors

N/A

Related Commands

- **show ip route** (route management)

1.43 ip ospf fast-reroute no-eligible-backup

Function

Run the **ip ospf fast-reroute no-eligible-backup** command to exclude an OSPF interface that cannot be used as a backup interface in the OSPF fast reroute calculation.

Run the **no** form of this command to restore the default configuration.

By default, an interface can be used as a backup interface of OSPF fast reroute.

Syntax

ip ospf fast-reroute no-eligible-backup

no ip ospf fast-reroute no-eligible-backup

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the remaining bandwidth of an interface is small or an interface may fail with the primary interface at the same time, the interface is not suitable for a backup interface. This command needs to be enabled in interface configuration mode of this interface. In the fast reroute calculation of OSPF, this interface is excluded and cannot be used as a backup interface, and a backup interface is selected from other interfaces. This command does not take effect if **fast-rerotue route-map** is configured.

Examples

The following example excludes GigabitEthernet 0/1 from being a backup interface in the fast reroute calculation of OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf fast-reroute no-eligible-backup
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (route management)

1.44 ip ospf hello-interval

Function

Run the **ip ospf hello-interval** command to configure the interval for OSPF to send hello packets.

Run the **no** form of this command to restore the default configuration.

By default, the hello packet interval is 10s for Ethernet, PPP, HDLC encapsulation interface, and frame relay point-to-point sub-interface. The hello packet interval is 30s for non-frame relay point-to-point sub-interface and X.25 interface.

Syntax

ip ospf hello-interval *hello-interval*

no ip ospf hello-interval

Parameter Description

hello-interval: Interval for OSPF to send hello packets, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The hello packet interval is contained in the hello packet. A shorter hello interval indicates that OSPF can detect topology changes more quickly, but the network traffic increases. The hello packet interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the hello packet interval.

Examples

The following example sets the interval for OSPF to send hello packets to 15s on the GigabitEthernet 0/1 interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15
```

Notifications

N/A

Common Errors

The hello packet intervals configured on different interfaces in the same area are inconsistent.

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.45 ip ospf message-digest-key

Function

Run the **ip ospf message-digest-key** command to configure a cipher text authentication key of OSPF packets.

Run the **no** form of this command to delete a configured cipher text authentication key of OSPF packets.

By default, no cipher text authentication key is configured.

Syntax

ip ospf message-digest-key *key-id* **md5** [**0** | **7**] *key*

no ip ospf message-digest-key *key-id*

Parameter Description

key-id: ID of the authentication key. The value range is from 1 to 255.

md5: Uses the MD5 cipher text authentication.

0: Indicates that the key is displayed in plain text.

7: Indicates that the key is displayed in cipher text.

key: The key, a string of up to 16 characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command configures a key of cipher text authentication, which takes effect only after the **area authentication** or **ip ospf authentication** command is used to configure the authentication type as **message-digest**. Authentication succeeds only when both *key-id* and key are matched.

Multiple *key-id* values are configured for the same interface, and the last *key-id* configured takes effect when packets are sent, but all *key-id* values can participate in the authentication when packets are received.

Examples

The following example configures the cipher text authentication of OSPF packets on the GigabitEthernet 0/1 interface as MD5, and key as hello.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf message-digest-key 10 md5 hello
```

Notifications

When a key not configured is deleted, the following notification will be displayed:

```
OSPF: Key 1 does not exist
```

When a configured key is configured again, the following notification will be displayed:

```
OSPF: Key 1 already exists
```

When a key is too long and will be truncated to 16 characters, the following notification will be displayed:

```
%OSPF: Warning: The password/key will be truncated to 16 characters
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **area authentication**
- **ip ospf authentication**

1.46 ip ospf mtu-ignore

Function

Run the **ip ospf mtu-ignore** command to disable MTU verification when an interface receives database description packets.

Run the **no** form of this command to enable MTU verification when an interface receives database description packets.

The MTU verification function is disabled by default.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When receiving a database description packet, OSPF verifies whether the MTU of the neighbor's interface is the same as that of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the neighbor relationship cannot be set up. To resolve this problem, you can disable MTU verification.

Examples

The following example disables MTU verification when the GigabitEthernet 0/1 interface receives database description packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 ip ospf network

Function

Run the **ip ospf network** command to configure the OSPF network type of an interface.

Run the **no** form of this command to restore the default configuration.

By default, the interface type of OSPF is not configured. No interface is set to P2MP type by default.

Syntax

ip ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** }

no ip ospf network

Parameter Description

broadcast: Sets the interface network type to **broadcast**.

non-broadcast: Sets the interface network type to non-broadcast multiple access (NBMA).

point-to-multipoint [**non-broadcast**]: Sets the interface network type to P2MP. If the interface does not have the broadcast capability, the **non-broadcast** parameter must be set.

point-to-point: Sets the interface network type to P2P.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The command is used to set a network type of OSPF according to the network topology. Ethernet and fiber distributed data interface (FDDI) fall into the broadcast type, X.25, frame relay, and ATM fall into the NBMA type, and PPP, HDLC, and LAPB fall into the P2P type. Each network type is restricted as follows:

- The broadcast type requires that the interface must have the broadcast capability.
- The P2P type requires that the interfaces are interconnected in one-to-one manner.
- The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.
- The P2MP type does not raise any requirement.

Examples

The following example configures the OSPF network type of the GigabitEthernet 0/1 interface as P2P type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-GigabitEthernet 0/1)#ip address 172.16.24.4 255.255.255.0
Hostname(config-GigabitEthernet 0/1)# encapsulation frame-relay
Hostname(config-GigabitEthernet 0/1)# ip ospf network point-to-point
```

The following example configures the OSPF network type of the GigabitEthernet 0/1 interface as NBMA.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-GigabitEthernet 0/1)# ip address 172.16.24.4 255.255.255.0
Hostname(config-GigabitEthernet 0/1)# encapsulation frame-relay
Hostname(config-GigabitEthernet 0/1)# ip ospf network non-broadcast
Hostname(config-GigabitEthernet 0/1)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.48 ip ospf priority

Function

Run the **ip ospf priority** command to configure the OSPF priority value of an interface.

Run the **no** form of this command to restore the default configuration.

The priority value is 1 by default.

Syntax

ip ospf priority *priority*

no ip ospf priority

Parameter Description

priority: OSPF priority value of an interface. The value range is from 0 to 255. A device with the priority 0 does not participate in the designated router (DR)/backup designated router (BDR) election.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The priority value of an OSPF interface is contained in the hello packet. When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does

not participate in the DR/BDR election. This command is applicable only to the OSPF broadcast and NBMA interfaces.

Examples

The following example configures the priority value of the GigabitEthernet 0/1 interface as **0**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf priority 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.49 ip ospf retransmit-interval

Function

Run the **ip ospf retransmit-interval** command to configure the retransmission interval of LSU packets on an interface.

Run the **no** form of this command to restore the default configuration.

The retransmission interval of LSU packets on an interface is 5s by default.

Syntax

ip ospf retransmit-interval *retransmit-interval*

no ip ospf retransmit-interval

Parameter Description

retransmit-interval: Retransmission interval of LSU packets, in seconds. This interval must be longer than the round-trip transmission delay of data packets between two neighbors. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet.

The retransmission interval can be set to a greater value on a serial line or virtual link to prevent unwanted retransmission. The LSU packet retransmission interval of a virtual link is defined using the **retransmit-interval** keyword in the **area virtual-link** command.

Examples

The following example sets the LSU packet retransmission interval on the GigabitEthernet 0/1 interface to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf retransmit-interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.50 ip ospf source-check-ignore

Function

Run the **ip ospf source-check-ignore** command to disable the source address verification function for the packets received on a P2P link.

Run the **no** form of this command to restore the default configuration.

The source address verification function for the packets received on a P2P link is enabled by default.

Syntax

ip ospf source-check-ignore

no ip ospf source-check-ignore

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information is notified during the P2P link negotiation, OSPF checks whether the source address of the packet is the address advertised by the peer end during negotiation. If not, OSPF determines that the packet is invalid and discards it. OSPF never verifies the address of an interface not configured with an IP address.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Examples

The following example configures that the Gigabit Ethernet 0/1 interface on the P2P link does not verify the source address of the received packet.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 ip ospf subvlan

Function

Run the **ip ospf subvlan** command to enable the OSPF function on a super VLAN.

Run the **no** form of this command to restore the default configuration.

By default, the OSPF function is disabled on a super VLAN.

Syntax

ip ospf subvlan [**all** | *vid*]

no ip ospf subvlan

Parameter Description

all: Allows sending packets to all sub VLANs.

vid: ID of the sub VLAN. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In normal cases, a super VLAN contains multiple sub VLANs. The corresponding OSPF multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the OSPF function does not need to be enabled on a super VLAN. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. Usually packets need to be sent to only one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the OSPF function on Super VLAN 300 and allows sending packets to Sub VLAN 1024.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# ip ospf subvlan 1024
```

Notifications

N/A

Common Errors

The function is configured on a non-super VLAN.

The specified sub VLAN on the super VLAN cannot implement interworking with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.52 ip ospf transmit-delay

Function

Run the **ip ospf transmit-delay** command to configure the delay for an OSPF interface to transmit LSU packets.

Run the **no** form of this command to restore the default configuration.

The LSU packet transmission delay is 1s by default.

Syntax

ip ospf transmit-delay *transmit-delay*

no ip ospf transmit-delay

Parameter Description

transmit-delay: Delay for an OSPF interface to transmit LSU packets, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before an LSU packet is transmitted, the **Age** fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmission delay and line propagation delay on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU packet transmission delay of a virtual link is configured through the **transmit-delay** option in the **area virtual-link** command.

If the value of the **Age** field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Examples

The following example sets the LSU packet transmission delay on the GigabitEthernet 0/1 interface to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip ospf transmit-delay 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.53 ispf enable

Function

Run the **ispf enable** command to enable the incremental shortest path first (iSPF) feature and run the iSPF algorithm to calculate the network topology.

Run the **no** form of this command to disable the iSPF feature.

The iSPF feature is disabled by default.

Syntax

ispf enable

no ispf enable

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

OSPF uses the classic shortest path first (SPF) algorithm to calculate the network topology information and routing information. Calculation of the topology information is based on the area, and the SPF algorithm runs independently in each area.

The iSPF algorithm is improved and optimized on the basis of SPF algorithm, and its calculation is still based on the area. However, after the network topology changes, the iSPF algorithm corrects only the nodes affected by the topology change, instead of re-building the entire shortest path tree (SPT). This accelerates OSPF convergence to a certain extent, and effectively relieves the load pressure of the device processor. Normally a larger network scale and a more complex structure show more significant advantages brought by the iSPF algorithm.

The iSPF algorithm does not involve interoperability with other devices, and devices on the same network can be configured differently. To speed up convergence of the entire network as much as possible, enable the iSPF feature for the devices throughout the network.

Enabling the iSPF feature influences only OSPF's selection of a network topology calculation algorithm. Therefore, the backoff time of route computation configured using the **timers spf** command and **timers throttle spf** command also takes effect for the iSPF algorithm.

Examples

The following example enables the iSPF feature.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# ispf enable
```

The following example enables the iSPF feature under VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1 vrf vpn1
Hostname(config-router)# ispf enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.54 log-adj-changes

Function

Run the **log-adj-changes** command to record the log of adjacency state changes.

Run the **no** form of this command to remove this configuration.

The log recording function is enabled by default, without the **detail** parameter.

Syntax

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

detail: Records all the state change information.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The log records the log information of the following four types of events only:

- The adjacency reaches the full state;
- The adjacency leaves the full state;
- The adjacency reaches the down state;
- The adjacency leaves the down state.

Examples

The following example records the log of adjacency state changes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# log-adj-changes detail
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.55 max-concurrent-dd

Function

Run the **max-concurrent-dd** command to configure the maximum number of neighbors with which the current OSPF process can concurrently initiate or accept interaction.

Run the **no** form of this command to restore the default configuration.

The maximum number of neighbors is 5 by default.

Syntax

max-concurrent-dd *neighbor-num*

no max-concurrent-dd

Parameter Description

neighbor-num: Maximum number of neighbors that concurrently interact with the OSPF process. The value range is from 1 to 65535.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which each OSPF process can concurrently initiate or accept interaction.

Examples

The following example configures the maximum number of neighbors with which the current OSPF process can concurrently initiate or accept interaction as 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10
Hostname(config-router)# max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.56 max-metric router-lsa

Function

Run the **max-metric router-lsa** command to configure the maximum advertisement metric of an OSPF-enabled device so that other routers will not preferably regard this router as a transmission node in SPF calculation.

Run the **no** form of this command to cancel the maximum advertisement metric.

By default, the LSAs of normal metric are advertised.

Syntax

max-metric router-lsa [**external-lsa** [*max-metric-value*] | **include-stub** | **on-neighborup** [*full-interval-time*] | **on-startup** [*startup-interval-time*] | **summary-lsa** [*max-metric-value*]] *

no max-metric router-lsa [**external-lsa** [*max-metric-value*] | **include-stub** | **on-neighborup** [*full-interval-time*] | **on-startup** [*startup-interval-time*] | **summary-lsa** [*max-metric-value*]] *

Parameter Description

router-lsa: Sets the metric of non-stub links in the router LSA to the maximum value (0xFFFF).

external-lsa: Allows a router to replace the metrics of external LSAs (including Type-5 and Type-7 LSAs) with the maximum metric.

max-metric-value: Maximum metric of the external LSA. The value range is from 1 to 16777215, and the default value is **16711680**.

include-stub: Sets the metrics of stub links in the router LSA advertised by the router to the maximum value.

on-startup: Allows a router to advertise the maximum metric when started.

startup-interval-time: The interval at which the maximum metric is advertised, in seconds. The value range is 5 to 86400, and the default value is **600**.

on-neighborup: Allows a router to advertise the maximum routing when its neighbor enters the full state.

full-interval-time: Interval at which the maximum metric is advertised, in seconds. The value range is 5 to 1800, and the default value is **120**.

summary-lsa: Allows a router to replace the metrics of summary LSAs (including Type-3 and Type-4 LSAs) with the maximum metric.

max-metric-value: Maximum metric of the summary LSA. The value range is from 1 to 16777215, and the default value is **16711680**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

After the **max-metric router-lsa** command is executed, the metrics of the non-stub links in the router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored.

By default, if this command is configured, the stub links still advertise the common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric.

- If an ABR does not wish to transfer inter-area traffic, run the **summary-lsa** parameter to set the metric of the summary LSA to the maximum metric.
- If an ASBR does not wish to transfer external traffic, run the **external-lsa** parameter to set the metric of the external LSA to the maximum metric.

The **max-metric router-lsa** command is generally used in the following scenarios:

- Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. If the current device is still building the BGP routing table and some BGP routes are not learned yet, packets sent to these networks are discarded. In this case, you can use the **on-startup** parameter to set a delay after which the restarted device acts as the transmission mode.
- Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic.
- Delete a device gracefully from the network. After the **max-metric router-lsa** command is configured, the

current device advertises the maximum metric among all the routes. In this way, other devices on the network can select the backup path for data transmission before the device is shut down.

- In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

Examples

The following example configures the maximum metric of non-stub links in the router LSAs as 100s when an OSPF-enabled router starts.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# max-metric router-lsa on-startup 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.57 neighbor

Function

Run the **neighbor** command to configure an OSPF neighbor.

Run the **no** form of this command to delete a specified neighbor.

An OSPF neighbor is disabled by default.

Syntax

neighbor *ipv4-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *priority*] *]

no neighbor *ipv4-address* [**cost** | [**poll-interval** | **priority**] *]

Parameter Description

ipv4-address: IP address of an interface on the neighbor.

cost *cost*: Indicates the cost required to reach each neighbor. This parameter is applicable only to the P2MP interface. The value range is from 0 to 65535.

poll-interval *poll-interval*: Indicates the neighbor polling interval, in seconds. This parameter is applicable only to the NBMA interface. The value range is 0 to 2147483647, and the default value is **120**.

priority *priority*: Indicates the neighbor priority value. This parameter is applicable only to the NBMA interface. The value range is from 0 to 255, and the default value is **0**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface.

If a neighbor router becomes inactive on the NBMA network, OSPF still sends hello packets to this neighbor even if no hello packet is received within the router failure time. The interval at which the hello packet is sent is called polling interval. When running for the first time, OSPF sends hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the hello packets to all neighbors to set up a neighbor relationship.

The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must run this command to manually configure neighbors for the P2MP (non-broadcast) network. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

Examples

The following example configures the IP address of an OSPF neighbor as 172.16.24.2, priority value as 1, and polling interval as 150s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# network 172.16.24.0 0.0.0.255 area 0
Hostname(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Notifications

When the configured neighbor address is the local address, the following notification will be displayed:

```
%OSPF: Warning: OSPF neighbor address 192.168.1.1 is our address
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf neighbor**

1.58 network area

Function

Run the **network area** command to configure which interfaces will run OSPF and which OSPF area they belong to.

Run the **no** form of this command to delete the OSPF area definition of an interface.

No interface IP address is configured to join the OSPF area by default.

Syntax

network *ipv4-address wildcard* **area** *area-id*

no network *ipv4-address wildcard* **area** *area-id*

Parameter Description

ipv4-address: IP address corresponding to the interface.

wildcard: IP address comparison bit. 0 indicates accurate matching, and 1 indicates that no comparison is performed.

area-id: ID of the OSPF area. The parameter can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To run OSPF on an interface, you can include the primary IP address of the interface in the IP address range defined by the **network area** command. By defining the *ipv4-address* and *wildcard* parameters, you can use one command to associate multiple interfaces with one OSPF area. If the interface address matches the IP address ranges defined in the **network area** command of multiple OSPF processes, the OSPF process that the interface is associated with is determined based on the optimal matching method.

If the IP address range defined by the **network area** command contains only the secondary IP address of the interface, OSPF does not run on this interface. You can also add an interface to an OSPF process using the **ip ospf area** command on the interface. If the **network area** command for the instance and the **ip ospf area** command on the interface are configured at the same time, the configuration on the interface takes effect first.

Examples

The following example configures three areas: 0, 1, and 172.16.16.0. The interface with an IP address in the range of 192.168.12.0/24 is defined to area 1, the interface with an IP address in the range of 172.16.16.0/20 is defined to Area 172.16.16.0, and the remaining interfaces are defined to Area 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# network 172.16.16.0 0.0.15.255 area 172.16.16.0
```

```
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 1
Hostname(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

Notifications

When an invalid address/mask combination is detected, the following notification will be displayed:

```
OSPF: Invalid address/mask combination
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**
- **show ip ospf database**

1.59 nsr

Function

Run the **nsr** command to configure the current OSPF process to support the non-stop routing (NSR) function.

Run the **no** form of this command to restore the default configuration.

The NSR function is disabled by default.

Syntax

nsr

no nsr

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

During NSR, OSPF-related information is backed up from the active supervisor module of a distributed device to the standby supervisor module, or from the active host of a virtual switching unit (VSU) to the standby host. In this way, the device can automatically recover the link state and re-generate routes without the help of the neighbor devices during the active/standby switchover. Information that should be backed up includes the neighbor relationship and link state.

For the same OSPF process, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is still supported.

The switchover of devices in distributed or VSU mode takes a period of time. If the OSPF neighbor keepalive duration is shorter than the switchover duration, the OSPF neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, you are advised to set the OSPF neighbor keepalive duration not less than the default value. When fast hello is enabled, the OSPF neighbor keepalive duration is less than 1s and the OSPF neighbor relationship times out during the switchover, causing NSR failures. Therefore, you are advised to disable fast hello when NSR is enabled.

Examples

The following example configures the current OSPF process 1 to support the NSR function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# nsr
```

Notifications

N/A

Common Errors

The neighbor keepalive duration is short. When fast hello is enabled, the OSPF neighbor relationship is removed during a switchover, causing forwarding interruption.

Platform Description

N/A

Related Commands

- **show ip ospf**

1.60 overflow database

Function

Run the **overflow database** command to configure the maximum number of LSAs supported by the current OSPF process.

Run the **no** form of this command to restore the default configuration.

The maximum number of LSAs is not configured by default.

Syntax

overflow database *max-lsa* [**hard** | **soft**]

no overflow database

Parameter Description

max-lsa: Maximum number of LSAs. The value range is from 1 to 4294967294.

hard: Indicates that the OSPF process will be stopped if the number of LSAs exceeds the limit.

soft: Indicates that a warning is generated when the number of LSAs exceeds the limit.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can configure the maximum number of LSAs supported by an OSPF process on a low performance device.

Examples

The following example configures the maximum number of LSAs supported by the current OSPF process as **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10
Hostname(config-router)# overflow database 10 hard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 overflow database external

Function

Run the **overflow database external** command to configure the maximum number of external LSAs and the waiting time for recovery from the overflow state to the normal state.

Run the **no** form of this command to restore the default configuration.

The maximum number of external LSAs is not configured by default.

If the maximum number of external LSAs is set, when the number of external LSAs exceeds the maximum, the normal state will not be restored.

Syntax

overflow database external *max-dbsize wait-time*

no overflow database external

Parameter Description

max-dbsize: Maximum number of external LSAs. This value must be the same on all the routers in the same AS. The value range is from 0 to 2147483647.

wait-time: Waiting time for a router in the overflow state to attempt to restore the normal state. The value range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can configure the maximum number of external LSAs on a low performance device. When the number of external LSAs of a device exceeds the configured *max-dbsize* value, the device enters the overflow state. In this state, the router no longer loads external LSAs and deletes external LSAs that are generated locally. After the set time of *wait-time* elapses, the device restores the normal state, and loads external LSAs again.

When using the **overflow database external** command, ensure that the same *max-dbsize* value is configured on all devices in the OSPF backbone area and common areas; otherwise, the following problems may occur:

- The LSDBs throughout the network are inconsistent, and the neighbor relationship fails to reach the full state.
- Routes are incorrect, including routing loops.
- AS external LSAs are frequently retransmitted.

Examples

The following example configures the maximum number of external LSAs as 10 and the waiting time for recovery from the overflow state to the normal state as 3s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10
Hostname(config-router)# overflow database external 10 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 overflow memory-lack

Function

Run the **overflow memory-lack** command to allow the OSPF process to enter the overflow state when the memory is insufficient.

Run the **no** form of this command to prevent the OSPF process from entering the overflow state when the memory is insufficient.

By default, the OSPF process is allowed to enter the overflow state when the memory is insufficient.

Syntax

overflow memory-lack

no overflow memory-lack

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively prevent the memory usage from increasing.

After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the occurrence probability of this problem, the OSPF process generates a default route to the null interface, and this route always exists in the overflow state.

You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state.

You can run the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

Examples

The following example prevents the OSPF process from entering the overflow state when the memory is insufficient.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# no overflow memory-lack
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 passive-interface

Function

Run the **passive-interface** command to configure a network interface specified for the local router as a passive interface.

Run the **no** form of this command to restore the default configuration.

By default, the passive modes of all interfaces are disabled, and all interfaces are allowed to send and receive OSPF packets.

Syntax

passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ipv4-address* }

no passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ipv4-address* }

Parameter Description

interface-type interface-number: Interface to be configured as a passive interface.

Default: Configures all interfaces as passive interfaces.

interface-type interface-number ipv4-address: Address of an interface as passive address.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or the specified IP address of a network interface as a passive address. The loopback interface and the interface of the unconnected OSPF neighbor can be set to passive interfaces.

Examples

The following example configures the GigabitEthernet 0/1 interface as a passive interface, and specifies the IP address 1.1.1.1 under the interface as a passive IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 30
Hostname(config-router)# passive-interface GigabitEthernet 0/1
Hostname(config-router)# passive-interface GigabitEthernet 0/1 1.1.1.1
```

Notifications

When an invalid interface is specified, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf interface**

1.64 redistribute

Function

Run the **redistribute** command to enable the function of redistributing the external routing information.

Run the **no** form of this command to disable the redistributing function.

The route redistribution function is not configured by default.

Syntax

redistribute { **arp-host** | **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** *metric-value* | **metric-type** { **1** | **2** } | **route-map** *route-map-name* | **subnets** | **tag** *tag-value*] *

no redistribute { **arp-host** | **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** | **metric-type** | **route-map** | **subnets** | **tag**] *

Parameter Description

arp-host: Indicates redistribution from host routes converted by ARP.

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

isis [*area-tag*]: Indicates redistribution from IS-IS. Here, *area-tag* specifies an IS-IS instance.

level-1 | **level-2** | **level-1-2**: Used only when IS-IS routes are redistributed. Only the routes of the specified level are redistributed. By default, only Level-2 IS-IS routes can be redistributed.

ospf *process-id*: Indicates redistribution from OSPF. Here, *process-id* specifies an OSPF process. The value range is from 1 to 65535.

match: Used only when OSPF routes are redistributed. Only the routes that match the specified criteria are redistributed. By default, all OSPF routes can be redistributed.

external [**1** | **2**]: Redistributes E1, E2, or all external routes.

internal: Redistributes internal routes and inter-area routes.

nssa-external [**1** | **2**]: Redistributes N1, N2, or all external routes of all NSSAs.

rip: Indicates redistribution from RIP.

static: Indicates redistribution from static routes.

metric *metric-value*: Sets the metric of an OSPF external LSA. The value range is from 0 to 16777214.

metric-type { **1** | **2** }: Sets the external route type to **E-1** or **E-2**.

route-map *route-map-name*: Sets the redistribution filtering rules. Here, the value of *route-map-name* cannot exceed 32 characters.

subnets: Specifies the non-standard networks for redistribution.

tag *tag-value*: Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value range is from 0 to 4294967295.

Command Modes

Routing configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type 5 LSAs to other OSPF routers in the domain.

If the **level** parameter is not carried when IS-IS route redistribution is configured, only Level-2 routes can be redistributed by default. The **level** parameter is carried during initial configuration of redistribution, the routes configured with the **level** parameter can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.

If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.

If **route-map** is specified, the **match** filtering rules specified in **route-map** are applicable to the original parameters of redistribution. For redistribution of OSPF or IS-IS routes, **route-map** is used for filtering only when the redistributed routes meet the criteria specified by **match** or **level**.

The **set metric** value of the associated **route-map** should fall into the range of 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

The configuration rules for the **no** form of the **redistribute** command are as follows:

- If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
- If no parameter is specified in the **no** form of this command, the entire command will be deleted.

For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level 2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

Examples

The following example configures to redistribute OSPF 2 and IS-IS isis-001 to OSPF1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# redistribute ospf 2 subnets
Hostname(config-router)# redistribute ospf 2 match external 1 internal
Hostname(config-router)# redistribute isis isis-001
Hostname(config-router)# redistribute isis isis-001 level-1
```

Notifications

When redistribution of this instance's routes is not allowed, the following notification will be displayed:

```
% Redistribution of "ospf 1" via "ospf 1" not allowed
```

When only classful network segments are redistributed, the following notification will be displayed:

```
% Only classful networks will be redistributed
```

Common Errors

The routes of the same OSPF process are redistributed.

Platform Description

N/A

Related Commands

- **show ip ospf database**

1.65 router ospf

Function

Run the **router ospf** command to create an OSPF routing process and enter routing configuration mode of OSPF.

Run the **no** form of this command to delete a created OSPF routing process.

The OSPF routing process is disabled by default.

Syntax

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf *process-id*

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535, and the default value is **1**.

vrf-name: VRF to which the OSPF process belongs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Based on the original implementation, the process ID parameter is added to the device software to realize expansion to a multi-instance OSPF process. Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently.

Examples

The following example creates an OSPF routing process in vrf vpn_1 and enters routing configuration mode of OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn_1
Hostname(config-router)#
```

Notifications

When no router ID can be allocated and the corresponding OSPF process cannot be started, the following notification will be displayed:

```
%OSPF-NORTRID: OSPF process 1 failed to allocate unique router-id and cannot start.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.66 router ospf max-concurrent-dd

Function

Run the **router ospf max-concurrent-dd** command to configure the maximum number of neighbors with which all the OSPF routing processes can concurrently initiate or accept interaction.

Run the **no** form of this command to restore the default configuration.

The maximum number of neighbors is **10** by default.

Syntax

router ospf max-concurrent-dd *max-neighbor*

no router ospf max-concurrent-dd

Parameter Description

max-neighbor: Maximum number of neighbors that concurrently interact with the OSPF process. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum number of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Examples

The following example configures the maximum number of neighbors with which all OSPF processes can concurrently initiate or accept interaction as **4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.67 router-id

Function

Run the **router-id** command to configure the ID of a router.

Run the **no** form of this command to delete the configured router ID and restore the default router ID.

By default, the OSPF routing process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPF process elects the largest one among the IP addresses of all its physical interfaces as the router ID.

Syntax

router-id *router-id*

no router-id

Parameter Description

router-id: Router ID to be configured, expressed in the form of an IP address.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

You can configure any IP address as the ID of the router, and ensure that the router ID is unique in an AS. After the router ID changes, OSPF performs a lot of internal processing. Therefore, you are advised to set the router ID before generating an LSA. When an attempt is made to modify the router ID, a prompt is displayed, requesting you to confirm the modification.

Examples

The following example configures the router ID as **0.0.0.36**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# router-id 0.0.0.36
```

Notifications

When you configure the router ID as **0.0.0.0** and this operation will stop the OSPF process, the following notification will be displayed:

```
% OSPF: router-id set to 0.0.0.0, process will not run.
```

When the configured router ID is duplicate with that of another process, the following notification will be displayed:

```
% OSPF: router-id 192.168.1.1 is in use by process 1
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.68 show ip ospf

Function

Run the **show ip ospf** command to display the summary of an OSPF process.

Syntax

show ip ospf [*process-id*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the summary of an OSPF process.

```
Hostname> enable
Hostname# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
  Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default
Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Enable ispf
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
   Condition: on startup for 100 seconds, State: inactive
   Advertise stub links with maximum metric in router-LSAs
   Advertise summary-LSAs with metric 16711680
   Advertise external-LSAs with metric 16711680
   Unset reason: timer expired, Originated for 100 seconds
   Unset time: 00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msecs
```

```
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
BFD enabled
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
iSPF algorithm executed 0 timesNumber of LSA 3. Checksum 0x0204bf
Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
iSPF algorithm executed 0 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled, Stability Interval expired in 00:00:03
```

Table 1-1 Output Fields of the show ip ospf Command

Field	Description
Router ID	Indicates the ID of a router.
Process uptime	Indicates the time when this OSPF process takes effect (the process is invalid when the router ID is 0.0.0.0).
Bound to VRF	Indicates the VRF to which the OSPF process belongs.
Conforms to RFC2328	Indicates conformity to RFC2328.

Field	Description
RFC1583Compatibility flag	Indicates whether the RFC1583 rule or RFC2328 rule is used in the external route computation; this rule will be used during selection of the optimal ASBR and route comparison.
Support Tos	Indicates that only TOS0 is supported.
Supports opaque LSA	Indicates that Opaque-LSA is supported.
Graceful-restart	Indicates the GR capability described by RFC3623 Graceful Restart.
Graceful-restart Helper	Indicates the GR helper capability described by RFC3623 Graceful Restart.
Router Type	Indicates that the OSPF router type is Normal, ABR, or ASBR.
SPF Delay	Indicates the required delay time before calling the SPF computation when a topology change is received.
SPF-holdtime	Indicates the minimum time of holding between two SPF calculations.
LsaGroupPacing	Indicates the interval between the LSA update, verification, computation, and aging operations.
Incomming current DD exchange neighbors	Indicates the number of neighbors in interaction. Incomming means that the neighbor enters the Exstart state for the first time.
Outgoing current DD exchange neighbors	Indicates the number of neighbors in interaction. Outgoing means that the neighbor returns from a higher state to the Exstart state for re-interaction.
Number of external LSA	Indicates the number of external LSAs stored in the database.
External LSA Checksum Sum	Indicates the sum of checksums of external LSAs stored in the database.
Number of opaque LSA	Indicates the number of Opaque-LSAs stored in the database.
Opaque LSA Checksum Sum	Indicates the sum of checksums of Opaque-LSAs stored in the database.
Number of non-default external LSA	Indicates the number of external LSAs of non-default routes.
External LSA database limit	Indicates the quantity limit of external LSAs.
Exit database overflow state interval	Judges the waiting time for a router to attempt to return to normal state from the overflow state.
Database overflow state	Indicates whether the current OSPF process is in the overflow state.
Number of LSA originated	Indicates the number of generated LSAs.

Field	Description
Number of LSA received	Indicates the number of received LSAs.
Log Neighbor Adjency Changes	Indicates whether the neighbor state change recording switch is enabled.
Number of areas attached to this router	Indicates the number of areas on this router.
Area type	Indicates the area type. The value can be Default, Stub, or NSSA.
Number of interfaces in this area	Indicates the number of interfaces in this area.
Number of fully adjacent neighbors in this area	Indicates the number of neighbors in full neighbor relationship in this area.
Number of fully adjacent virtual neighbors through this area	Indicates the number of neighbors of virtual links with two neighbors already in the full state in this area. This field is valid only for the non-backbone area of default type.
Area authentication	Indicates the area authentication method.
SPF algorithm last executed	Indicates the duration from the last SPF computation to the present time.
SPF algorithm executed times	Indicates the SPF computation times.
Number of LSA	Indicates the total number of LSAs in this area.
Checksum Sum	Indicates the sum of the checksums of LSAs in this area.
NSSA Translator State	Indicates whether the NSSA LSA is converted to an external LSA. This field is valid only for the OSPF process that is an ABR in the NSSA.
BFD enabled	Indicates that correlating OSPF with BFD is enabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.69 show ip ospf border-routers

Function

Run the **show ip ospf border-routers** command to display the OSPF internal routing table to an ABR/ASBR.

Syntax

show ip ospf [*process-id*] **border-routers**

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command can be used to display the OSPF internal route to an ABR or ASBR. The OSPF internal routing table is different from the routing table displayed using the **show ip route** command. The target address of the OSPF internal routing table is the OSPF router ID, not the target network.

Examples

The following example displays the OSPF internal routing table to an ABR/ASBR.

```
Hostname> enable
Hostname# show ip ospf border-routers
OSPF internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, GigabitEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
```

Table 1-2 Output Fields of the show ip ospf border-routers Command

Field	Description
Codes	Indicates the route type code definition. Here, i indicates an internal route of the area, and I indicates a route between areas.
i	Indicates that this route is an internal route of the area.
1.1.1.1	Displays the OSPF ID of the boundary router.
[2]	Displays the cost value to the boundary router.
via 10.0.0.1	Displays the next hop gateway to the boundary router.
GigabitEthernet 0/1	Displays the interface to the boundary router.
ABR, ASBR	Displays the type of the boundary router: ABR or ASBR, or both.
Area 0.0.0.1	Displays the area where the route is learned.
select	Indicates the optimum path currently selected when multiple paths are available to the ASBR.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.70 show ip ospf database

Function

Run the **show ip ospf database** command to display the information of an OSPF LSDB.

Syntax

show ip ospf [*process-id* [*area-id* [*ipv4-address*]]] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** *ipv4-address* | **self-originate** } | *link-state-id* | **brief**] [**database-summary** | **max-age** | **detail**]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area-id: ID of the OSPF area, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

ipv4-address: ID of the OSPF area, which is an IP address, for example, 0.0.0.1.

adv-router: Displays the link state description information generated by the specified adverting router.

link-state-id: Link state description information of the specified OSPF link state ID to be displayed.

self-originate: Displays the link state description information generated by the local router.

max-age: Displays the LSA whose aging time expires.

router: Displays the link state description information of the OSPF router.

network: Displays the link state description information of the OSPF network.

summary: Displays the link state description summary of the OSPF link.

asbr-summary: Displays the link state description summary of the ASBR.

external: Displays the external link state description of the OSPF process.

nssa-external: Displays the Type-7 external link state description of the OSPF process.

opaque-area: Displays the Type-10 LSA.

opaque-as: Displays the Type-11 LSA.

opaque-link: Displays the Type-9 LSA.

database-summary: Displays the statistical summary of each type of LSA in the OSPF LSDB.

detail: Displays the details about all LSAs of the OSPF process.

brief: Displays the summary of the specified type of LSA.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the OSPF LSDB is large, itemized display is necessary. Correct use of these commands is helpful to the troubleshooting of OSPF faults.

Examples

The following example displays the information about the OSPF LSDB.

```
Hostname> enable
Hostname# show ip ospf database
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#      CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000011 0x6f39 2
3.3.3.3        3.3.3.3        120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#      CkSum
192.88.88.27    1.1.1.1        120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#      CkSum  Route
10.0.0.0       1.1.1.1        2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0      1.1.1.1        2    0x8000000c 0x1ecb 100.0.0.0/16
Router Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Router     Age  Seq#      CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000001 0x91a2 1
Summary Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Router     Age  Seq#      CkSum  Route
100.0.0.0      1.1.1.1        2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0    1.1.1.1        2    0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID    ADV Router    Age  Seq#      CkSum  Route          Tag
20.0.0.0    1.1.1.1     1    0x80000001 0x033c E2 20.0.0.0/24  0
100.0.0.0  1.1.1.1      1    0x80000001 0x9469 E2 100.0.0.0/28 0
AS External Link States
Link ID   ADV Router    Age  Seq#      CkSum  Route          Tag
20.0.0.0  1.1.1.1       380  0x8000000a 0x7627 E2 20.0.0.0/24  0
100.0.0.0   1.1.1.1     620  0x8000000a 0x0854 E2 100.0.0.0/28 0
```

Table 1-3 Output Fields of the show ip ospf database Command

Field	Description
OSPF Router with ID	Displays the process ID of the OSPF LSDB's router ID that corresponds to this OSPF process.
Router Link States	Indicates that the following content is the link state description of the router.
Net Link States	Indicates that the following content is the network link state description.
Summary Net Link States	Indicates that the following content is the network link state description summary.
NSSA-external Link States	Indicates that the following content is the external link state description of Type-7 AS.
AS External Link States	Indicates that the following content is the external link state description of Type-5 AS.
Link ID	Indicates the link ID.
ADV Router	Indicates the ID of the router that advertises the link state description.
Age	Displays the keeping time of the link state description.
Seq#	Displays the sequence number of the link state description, used to detect the old or duplicate LSA.
Cksum	Displays the checksum of the link state description.
Link-Count	Displays the number of links in the link state description information of the router.
Route	Displays the route information contained in the LSA.
Tag	Displays the tag of the link state description.

The following example displays the link state description summary of an ASBR.

```
Hostname> enable
Hostname# show ip ospf database asbr-summary
OSPF Router with ID (1.1.1.35) (Process ID 1)
ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Router address)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
```

```
TOS: 0  Metric: 1
```

Table 1-4 Output Fields of the show ip ospf database asbr-summary Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
AS Summary Link States	Indicates that the following content displays the link description summary of the AS.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Network Mask	Displays the subnet mask of the route corresponding to the link state description.
TOS	Indicates the TOS value, which can only be 0 at present.
Metric	Displays the metric value of the route corresponding to the link state description.

The following example displays the external link state description of the OSPF process.

```
Hostname> enable
Hostname# show ip ospf database external
OSPF Router with ID (1.1.1.35) (Process ID 1)
AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
```

```
Forward Address: 0.0.0.0
External Route Tag: 0
```

Table 1-5 Output Fields of the show ip ospf database external Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
Type-5 AS External Link States	Indicates that the following content is the external link state description of the AS.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Network Mask	Displays the subnet mask of the route corresponding to the link state description.
Metric Type	Indicates the external link type.
TOS	Indicates the TOS value, which can only be 0 at present.
Metric	Displays the metric value of the route corresponding to the link state description.
Forward Address	Indicates that the data traffic to the target network will be forwarded to this IP address. If the address is 0.0.0.0, the data traffic will be forwarded to the router that generates this link state.
External Route Tag	Indicates the external route tag. Every external route has a 32-bit route tag. The OSPF process does not use this route tag, which will be used when other routing processes redistribute OSPF routes.

The following example displays the link state description of the OSPF network.

```
Hostname> enable
Hostname# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
```

```
Options: 0x2 (*|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.88.88.27 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x5366
Length: 32
Network Mask: /24
Attached Router: 1.1.1.1
Attached Router: 3.3.3.3
```

Table 1-6 Output Fields of the show ip ospf database network Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
Network Link States	Indicates that the following content is the network link state description.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Network Mask	Displays the subnet mask of the network corresponding to the link state description.
Attached Router	Displays the routers connected on the network.

The following example displays the link state description of the OSPF router.

```
Hostname> enable
Hostname# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
Options: 0x2 (*|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 1.1.1.1
```

```
Advertising Router: 1.1.1.1
LS Seq Number: 80000012
Checksum: 0x6d3a
Length: 48
Number of Links: 2
Link connected to: Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

Table 1-7 Output Fields of the show ip ospf database router Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
Router Link States	Indicates that the following content is the link state description of the router.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
Flag	Indicates the router flag.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Number of Links	Displays the number of links associated with the router.
Link connected to	Displays the device to which the link is connected and the type of the network.
(Link ID)	Indicates the link ID.
(Link Data)	Indicates the link data.
Number of TOS metrics	Indicates the TOS value, which is 0.
TOS 0 Metrics	Indicates the metric value of TOS 0.

The following example displays the link state description summary of the OSPF process.

```
Hostname> enable
```

```
Hostname# show ip ospf database summary
OSPF Router with ID (1.1.1.1) (Process ID 1)
Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
TOS: 0  Metric: 11
```

Table 1-8 Output Fields of the show ip ospf database summary Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
Summary Net Link States	Indicates that the following content is the network link state description summary.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Network Mask	Displays the subnet mask of the route corresponding to the link state description.
TOS	Indicates the TOS value, which can only be 0 at present.
Metric	Displays the metric value of the route corresponding to the link state description.

The following example displays the Type-7 external link state description of the OSPF process.

```
Hostname> enable
Hostname# show ip ospf database nssa-external
OSPF Router with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
```

```
LS age: 1
Options: 0x0 (*|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
NSSA: Forward Address: 100.0.2.1
External Route Tag: 0
```

Table 1-9 Output Fields of the show ip ospf database nssa-external Command

Field	Description
OSPF Router with ID	Indicates the router ID corresponding to the following information and the corresponding ID of this OSPF process.
NSSA-external Link States	Indicates that the following content is the external link state description of the Type-7 AS.
LS age	Displays the keeping time of the link state description.
Options	Indicates the options.
LS Type	Displays the type of the link state description.
Link State ID	Displays the link ID of the link state description.
Advertising Router	Indicates the advertising router of the link state description.
LS Seq Number	Displays the sequence number of the link state description.
Checksum	Displays the checksum of the link state description.
Length	Displays the length of the link state description, in bytes.
Network Mask	Displays the subnet mask of the route corresponding to the link state description.
Metric Type	Indicates the external link type.
TOS	Indicates the TOS value, which can only be 0 at present.
Metric	Displays the metric value of the route corresponding to the link state description.
NSSA:Forward Address	Indicates that the data traffic to the target network will be forwarded to this IP address. If the address is 0.0.0.0, the data traffic will be forwarded to the router that generates this link state.

Field	Description
External Route Tag	Indicates the external route tag. Every external route has a 32-bit route tag. The OSPF process does not use this route tag, which will be used when other routing processes redistribute OSPF routes.

The following example displays the statistical summary of each type of LSA in the OSPF LSDB.

```
Hostname> enable
Hostname# show ip ospf database database-summary
OSPF process 1:
Router Link States      : 4
Network Link States     : 2
Summary Link States     : 4
ASBR-Summary Link States : 0
AS External Link States  : 4
NSSA-external Link States: 2
```

Table 1-10 Output Fields of the show ip ospf database database-summary Command

Field	Description
OSPF Process	Displays the routing process ID corresponding to the following information.
Router Link	Indicates the number of OSPF router LSAs in this area.
Network Link	Indicates the number of OSPF network LSAs in this area.
Summary Link	Indicates the number of OSPF network summary LSAs in this area.
ASBR-Summary Link	Indicates the number of OSPF ASBR summary LSAs in this area.
AS External Link	Indicates the number of OSPF external LSAs in this area.
NSSA-external Link	Indicates the number of OSPF NSSA LSAs in the router.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.71 show ip ospf interface

Function

Run the **show ip ospf interface** command to display the information about an interface associated with an OSPF process.

Syntax

show ip ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

interface-type interface-number: Specified interface.

brief: Displays the brief information of the interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command can display the interfaces where OSPF runs, and the configuration information of these interfaces that related to the OSPF process.

Examples

The following example displays the information about the interface associated with the OSPF process.

```
Hostname> enable
Hostname# show ip ospf interface GigabitEthernet 0/1
GigabitEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1,
BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

Table 1-11 Output Fields of the show ip ospf interface GigabitEthernet 0/1 Command

Field	Description
GigabitEthernet 0/1 State	Indicates the state of the network interface: Up indicates normal operation, and Down indicates a fault.
Internet Address	Indicates the IP address of the interface.
Area	Indicates the OSPF area to which the interface belongs.
MTU	Indicates the corresponding MTU.
Matching network config	Indicates the configuration for the **network area** command corresponding to the OSPF process.
Process ID	Indicates the corresponding process ID.
Router ID	Indicates the ID of the OSPF router.
Network Type	Indicates the OSPF network type.
Cost	Indicates the cost of the OSPF interface.
Transmit Delay is	Indicates the transmission delay of the OSPF interface.
State	Indicates the DR/BDR state ID.
Priority	Indicates the priority of this interface.
Designated Router(ID)	Indicates the ID for the DR of this interface.
DR's Interface address	Indicates the interface address for the DR of this interface.
Backup designated router(ID)	Indicates the ID for the BDR of this interface.
BDR's Interface address	Indicates the interface address for the BDR of this interface.
Time intervals configured	Indicates the Hello, Dead, Wait, and Retransmit time corresponding to this interface.
Hello due in	Indicates the last time of sending a hello packet.
Neighbor count	Indicates the total number of neighbors.
Adjacent neighbor count	Indicates the number of neighbors in full neighbor relationship.
Crypt Sequence Number	Indicates the sequence number of MD5 authentication corresponding to this interface.
Hello received send	Indicates the statistics of the received and sent hello packets.
DD received send	Indicates the statistics of the received and sent DD packets.
LS-Req received send	Indicates the statistics of the received and sent LS request packets.

Field	Description
LS-Upd received send	Indicates the statistics of the received and sent LS update packets.
LS-Ack received send	Indicates the statistics of the received and sent LS response packets.
Discard	Indicates the statistics of the discarded OSPF packets.
BFD enabled	Indicates that correlating OSPF with BFD is enabled.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.72 show ip ospf ispf

Function

Run the **show ip ospf ispf** command to display the times of route computation through iSPF in the OSPF area.

Syntax

show ip ospf [*process-id*] **ispf**

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the times of route computation through iSPF in the OSPF area in the last 30 minutes, as well as the total times of computation using the iSPF algorithm up to now.

Examples

The following example displays the times of iSPF computation in the OSPF area.

```
Hostname> enable
Hostname# show ip ospf 1 ispf
OSPF process 1:
Area_id     30min_counts   Total_counts
```

```
0           32          1235
1           6           356
```

Table 1-12 Output Fields of the show ip ospf 1 ispf Command

Field	Description
Area_id	Indicates the OSPF area ID.
30min_counts	Indicates the times of iSPF computation in the last 30 minutes.
Total_counts	Indicates the total times of iSPF computation up to now.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.73 show ip ospf neighbor

Function

Run the **show ip ospf neighbor** command to display the neighbor table of an OSPF process.

Syntax

show ip ospf [*process-id*] **neighbor** [[*interface-type interface-number* | *neighbor-id*] * [**detail**] | **statistics**]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

interface-type interface-number: Neighbor information of a specified interface.

neighbor-id: Information about a specified neighbor.

detail: Displays the neighbor details.

statistics: Displays the statistics of neighbors.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command can be used to display the neighbor information and confirm whether the OSPF process is running normally.

Examples

The following example displays the neighbor list of an OSPF process.

```
Hostname> enable
Hostname# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State    BFD State   Dead Time   Address       Interface
3.3.3.3      1    Full/BDR  Up        00:00:32   192.88.88.72   GigabitEthernet
0/1
Hostname# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface GigabitEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
BFD session state up
```

Table 1-13 Output Fields of the show ip ospf neighbor Command

Field	Description
Neighbor ID	Indicates the ID of the neighbor router.
Pri	Indicates the priority (used to elect a DR) of the neighbor.
State	Indicates the state of the neighbor.
Dead Time	Indicates the time before the neighbor enters the dead state.
Address	Indicates the IP address of the interface corresponding to the neighbor.
Interface	Indicates the interface corresponding to the neighbor.
interface address	Indicates the interface address of the neighbor router.
In the area	Displays the area where the neighbor is learned.
via interface	Displays the interface where the neighbor is learned.

Field	Description
Neighbor priority	Indicates the priority value of the neighbor.
State	Indicates the connection state of the OSPF neighbor. DR or BDR is unavailable for the point-to-point network type. ● **Full** indicates the stable state. ● **DR** indicates that the neighbor is the specified router. ● **BDR** indicates that the neighbor is the specified router for backup. ● **DROTHER** indicates that the neighbor is not a DR/BDR.
State changes times	Indicates the change times of the neighbor state.
Dead Time	Displays the time when the dead state of this neighbor is declared.
DR	Indicates the interface address (namely, the DR field of the hello packet) of the DR elected by the neighbor router.
BDR	Indicates the interface address (namely, the BDR field of the hello packet) of the BDR elected by the neighbor router.
Options	Indicates the option for the E bit of the hello packet: ● **0** indicates that the area is a stub area. ● **2** indicates that the area is not a stub area.
Dead timer due in	Indicates the time before the neighbor router enters the dead state.
Neighbor up time	Indicates the duration from the time of discovering the neighbor router to the current time.
Database Summary List	Indicates the DD packet statistics of the neighbor.
Link State Request List	Indicates the LS request packet statistics of the neighbor.
Link State Retransmission List	Indicates the retransmitted packet statistics of the neighbor.
Crypt Sequence Number	Indicates the MD5 authentication code of the area.
Thread Inactivity Timer	Indicates the inactivity timer state of the neighbor.
Thread Database Description Retransmission	Indicates the DD packet timer state of the interface.
Thread Link State Request Retransmission	Indicates the LS request packet timer state of the interface.
Thread Link State Update Retransmission	Indicates the LS update packet timer state of the interface.
Thread Poll Timer	Indicates the poll timer startup state of the statically configured neighbor.

Field	Description
Graceful-restart Helper	Indicates whether the local router can become a GR helper for the specified neighbor.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.74 show ip ospf route

Function

Run the **show ip ospf route** command to display an OSPF route.

Syntax

show ip ospf [*process-id*] **route** [**count** | *ipv4-address mask*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

count: Displays the statistics of all kinds of OSPF routes.

ipv4-address mask: Routing information of the specified prefix and mask.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays an OSPF route.

```
Hostname> enable
Hostname# show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, B – Backup, O - OSPF,
IA - OSPF inter area  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
E2 100.0.0.0/24 [1/20] via 192.88.88.126, GigabitEthernet 0/1
B                  via 192.88.89.126, GigabitEthernet 0/2
C  192.88.88.0/24 [1] is directly connected,GigabitEthernet 0/1,Area 0.0.0.1
```

Table 1-14 Output Fields of the show ip ospf neighbor Command

Field	Description
codes	Indicates the route type and corresponding abbreviation description.
100.0.0.0/24	Indicates the corresponding prefix of the route.
[1/20]	Indicates the management distance and cost value corresponding to the route.
via	Indicates the next hop and interlace of the route.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.75 show ip ospf sham-links

Function

Run the **show ip ospf sham-links** command to display the sham link information of an OSPF process.

Syntax

show ip ospf [*process-id*] **sham-links** [**area** *area-id*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area *area-id*: Indicates the ID of the OSPF area where the sham link is, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the sham link information of an OSPF process.

```
Hostname> enable
Hostname# show ip ospf sham-links
Sham Link SLINK1 to address 8.8.8.8 is up
  Area 0.0.0.0 source address 7.7.7.7, Cost: 10
  Output interface is GigabitEthernet 0/8
  Nexthop address 192.168.1.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency state Full
```

Table 1-15 Output Fields of the show ip ospf sham-links Command

Field	Description
Area	Indicates the domain ID.
source address	Indicates the source IP address of the sham link.
Cost	Indicates the cost value of the sham link.
Output interface	Indicates the actual outbound interface of the sham link.
Nexthop address	Indicates the actual next-hop address of the sham link.
Transmit Delay	Indicates the transmission delay of the sham link.
State	Indicates the state of the sham link.
Time intervals configured	Indicates the Hello, Dead, Wait, and Retransmit time corresponding to the sham link.
Adjacency State	Indicates the adjacency state. **Full** indicates the stable state.

Notifications

If the specified OSPF process does not exist (for example, when the sham link information of OSPF 1 is checked), the following notification will be displayed:

```
%OSPF: No router process 1
```

Platform Description

N/A

Related Commands

N/A

1.76 show ip ospf spf

Function

Run the **show ip ospf spf** command to display the times of route computation in the OSPF area.

Syntax

show ip ospf [*process-id*] **spf**

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the times of route computation in the OSPF area in the last 30 minutes, as well as the total times of route computation up to now.

Examples

The following example displays the times of route computation in the OSPF area.

```
Hostname> enable
Hostname# show ip ospf 1 spf
OSPF process 1:
Area_id     30min_counts   Total_counts
0           32             1235
1           6              356
```

Table 1-16 Output Fields of the show ip ospf 1 spf Command

Field	Description
Area_id	Indicates the OSPF area ID.
30min_counts	Indicates the times of route computation in the OSPF area in the last 30 minutes.
Total_counts	Indicates the total times of route computation in the OSPF area up to now.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.77 show ip ospf summary-address

Function

Run the **show ip ospf summary-address** command to display the summarized route of all the redistributed routes of an OSPF process.

Syntax

show ip ospf [*process-id*] **summary-address**

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Currently this command takes effect only on an ABR of NSSA, and it displays only the route that is summarized on the local device.

Examples

The following example displays the summarized route of all the redistributed routes of an OSPF process.

```
Hostname> enable
Hostname# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise
```

Table 1-17 Output Fields of the show ip ospf summary-address Command

Field	Description
Summary Address	Indicates the address of the route to be summarized.
Summary Mask	Indicates the subnet mask of the route to be summarized.
Advertise	Indicates whether to advertise the summarized route.
Status	Indicates whether the range of the route to be summarized takes effect.
Aggregated subnets	Indicates how many external routes are summarized in this range.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.78 show ip ospf topology

Function

Run the **show ip ospf topology** command to display the topology information of SPF computation of an OSPF process.

Syntax

show ip ospf [*process-id* [*area-id*]] **topology**

[**adv-router** *adv-router-id* [*router-id*] | **self-originate** [*router-id*]]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

topology: Displays the topology summary of a specified OSPF process and area.

adv-router: Displays the topology information of a specified device, which must be a direct neighbor of the current device.

adv-router-id: Root node router ID of the shortest path tree.

router-id: Information about a specified node on the shortest path tree.

self-originate: Displays the topology information of the current device.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command helps users to learn the topology information of OSPF SPF computation, and locate the faults caused by topology planning. If a user has enabled fast reroute calculation, the command displays the information about fast reroute calculation.

Examples

The following example displays the topology summary of a specified OSPF process and area.

```
Hostname> enable
Hostname# show ip ospf topology
```

```
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Topology States (Area 0.0.0.0)
+1.1.1.1
  +2.2.2.2
    +4.4.4.4
  +3.3.3.3
    +4.4.4.4
+2.2.2.2
  +1.1.1.1
    +3.3.3.3
  +4.4.4.4
    +3.3.3.3
+3.3.3.3
  +1.1.1.1
    +2.2.2.2
  +4.4.4.4
    +2.2.2.2
```

The following example displays the topology information of the current device.

```
Hostname> enable
Hostname# show ip ospf topology self-originate
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Topology States (Area 0.0.0.0)
1.1.1.1
  Self to Destination Metric: 0
Parent Node:
Child Node:2.2.2.2
  Primary next-hop:
  Backup next-hop:
  Backup Neighbor:
2.2.2.2
  Self to Destination Metric: 1
Parent Node: 1.1.1.1
Child Node:
  Primary next-hop: GigabitEthernet 0/1 via 10.0.0.1
  Backup next-hop: GigabitEthernet 0/2 via 10.0.1.1
  Backup Neighbor: 2.2.2.2
Neighbor to Destination Metric: 0
Neighbor to Self Metric: 10
Neighbor to Primary Neighbor: 0
Self to Neighbor Metric: 1
```

Table 1-18 Output Fields of the show ip ospf topology Command

Field	Description
Self to Destination Metric	Indicates the metric from the root node to the current destination node.

Field	Description
Parent Node	Indicates the parent node of the current destination node.
Child Node	Indicates the child node of the current destination node.
Primary next-hop	Reaches the primary next hop of the current destination node.
Backup next-hop	Reaches the backup next hop of the current destination node.
Backup Neighbor	Reaches the backup neighbor of the current destination node.
Neighbor to Destination Metric	Indicates the metric from the backup neighbor to the current destination node.
Neighbor to Self Metric	Indicates the metric from the backup neighbor to the root node.
Neighbor to Primary Neighbor	Indicates the metric from the backup neighbor to the primary neighbor.
Self to Neighbor Metric	Indicates the metric from the root node to the backup neighbor.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.79 show ip ospf virtual-links

Function

Run the **show ip ospf virtual-links** command to display the information about a virtual link of an OSPF process.

Syntax

show ip ospf [*process-id*] **virtual-links** [*ipv4-address*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

ipv4-address: Router ID of the neighbor of a virtual link.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If a virtual link is configured, the neighbor state and other related information can be displayed only by running this command. The **show ip ospf neighbor** command does not display the neighbors of the virtual link.

Examples

The following example displays the information about a virtual link of an OSPF process.

```
Hostname> enable
Hostname# show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface GigabitEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

Field description:

Field	Description
Virtual Link VLINK0 to router	Displays the neighbor and neighbor state of the virtual link.
Virtual Link state	Displays the state of the virtual link.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the interface associated with the virtual link.
Local address	Indicates the address of the local interface.
Remote Address	Indicates the address of the peer interface.
Transmit Delay	Displays the transit delay of the virtual link.
State	Indicates the link state.
Time intervals configured	Indicates the Hello, Dead, Wait, and Retransmit time corresponding to this interface.
Adjacency State	Indicates the adjacency state. **Full** indicates the stable state.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.80 show running-config router ospf

Function

Run the **show running-config router ospf** command to display the configuration of an OSPF process.

Syntax

show running-config router ospf

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of an OSPF process.

```
Hostname> enable
Hostname# show running-config router ospf
router ospf 1
 router-id 1.1.1.1
 graceful-restart
 network 10.1.1.0 0.0.0.255 area 0
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.81 summary-address

Function

Run the **summary-address** command to configure a summarized route for the external routes of the OSPF routing domain.

Run the **no** form of this command to delete the definition of summarized route.

The route summarization function is disabled by default.

Syntax

summary-address *ipv4-address mask* [[**cost** *cost* | **distribute-delay** *interval* | **nssa-only** | **tag** *tag-value*] * | **not-advertise**]

no summary-address *ipv4-address mask* [[**cost** | **distribute-delay** | **nssa-only** | **tag**] * | **not-advertise**]

Parameter Description

ipv4-address: IP address of the summarized route.

mask: Subnet mask of the summarized route.

cost *cost*: Set the cost value of the summarized route. The value range is from 0 to 16777214. If no cost value is configured, the default metric of the summarized route is related to compatibility with RFC1583. If the RFC1583 compatibility mode is configured, the default metric is the minimum cost value of the summarized route; otherwise, the default metric is the maximum cost value of the summarized route.

distribute-delay *interval*: Specifies the delay time after which the summarized route is advertised, in seconds. The value range is 1 to 65535, and the default value is **2**.

nssa-only: Specifies that the summarized route cannot be converted to a Type-5 route. By default, the summarized route can be converted to a Type-5 route.

tag *tag-value*: Sets the tag value of the summarized route. The value range is from 0 to 4294967295.

not-advertise: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When routes are redistributed from other routing processes and injected to the OSPF routing process, each route is advertised to the OSPF routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertise only one summarized route to reduce the size of the routing table.

When configured on the NSSA ABR translator, the **summary-address** command summarizes the redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), this command summarizes only the redistributed routes. The **area range** command summarizes the routes between OSPF areas, while the **summary-address** command summarizes the external routes of the OSPF routing domain.

Examples

The following example configures a summarized route for the external routes of the OSPF routing domain as 100.100.0.0/16.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# summary-address 100.100.0.0 255.255.0.0
Hostname(config-router)# redistribute static subnets
Hostname(config-router)# network 200.2.2.0 0.0.0.255 area 1
Hostname(config-router)# network 172.16.24.0 0.0.0.255 area 0
Hostname(config-router)# area 1 nssa
```

Notifications

When an invalid mask is configured, the following notification will be displayed:

```
OSPF: Invalid mask input
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf summary-address**

1.82 timers lsa arrival

Function

Run the **timers lsa arrival** command to configure the delay for receiving a duplicate LSA.

Run the **no** form of this command to restore the default configuration.

By default, the delay for receiving a duplicate LSA is 1000 ms.

Syntax

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

arrival-time: Delay after which a duplicate LSA is received, in milliseconds. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Using this command can avoid consuming the device resource and the duplicate LSA received within a specified time does not need to be processed.

Examples

The following example configures the delay after which a duplicate LSA is received as 2s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# timers lsa arrival 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.83 timers pacing lsa-group

Function

Run the **timers pacing lsa-group** command to configure a group pacing interval of LSA.

Run the **no** form of this command to restore the default configuration.

The group pacing interval of LSA is 30s by default.

Syntax

timers pacing lsa-group *pacing-interval*

no timers pacing lsa-group

Parameter Description

update-time: Group pacing interval of LSA, in seconds. The range is from 10 to 1800.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Every LSA has its time to live (LSA age). When the LSA age reaches 3,600s, a refreshment is needed to prevent normal LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. To use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called

group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole.

If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. For CPU stability, the number of LSAs processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval. If there are 40 to 100 LSAs only, you can set the pacing interval to 10-20 minutes.

Examples

The following example configures the group pacing interval of LSA as 120s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# timers pacing lsa-group 120
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.84 timers pacing lsa-transmit

Function

Run the **timers pacing lsa-transmit** command to configure an interval for sending LSA group and a number of LS-UPD packets in each group.

Run the **no** form of this command to restore the default configuration.

By default, the interval for sending LSA group is 40 ms, and the number of LS-UPD packets in each group is 1.

Syntax

timers pacing lsa-transmit *transmit-interval transmit-count*

no timers pacing lsa-transmit

Parameter Description

transmit-interval: Interval of sending LSA group packets, in milliseconds. The value range is from 10 to 1000.

transmit-count: Number of LS-UPD packets in each group. The value range is from 1 to 200.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the number of LSAs is large and the device load is heavy in an environment, configuring an appropriate interval of sending LSA group and an appropriate number of LS-UPD packets in each group can limit the number of LS-UPD packets flooded on a network.

If the CPU usage is not high and the network bandwidth load is not heavy, reducing the interval of sending LSA group and increasing the number of LS-UPD packets in each group can accelerate the environment convergence.

Examples

The following example configures the interval for sending LSA group as 50 ms, and the number of LS-UPD packets in each group as 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# timers pacing lsa-transmit 50 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.85 timers spf

Function

Run the **timers spf** command to configure the delay time for SPF computation after an OSPF process receives the topology change information and the time interval between two SPF computations.

Run the **no** form of this command to restore the default configuration.

By default, the **timers spf** command does not take effect, and the delay for SPF computation is subject to the default configuration of the **timers throttle spf** command. Refer to the description of the **timers throttle spf** command.

Syntax

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

spf-delay: Delay for SPF computation, in seconds. After receiving the topology change information, the OSPF routing process must wait for the specified time before performing SPF computation. The range is from 0 to 2147483647.

spf-holdtime: Interval between two SPF computations, in seconds. If the waiting time expires, but the interval between two computations does not time out, the SPF computation cannot start. The range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Changes to LSDB trigger SPF computation. Frequent network jitter consumes a lot of CPU resources. Setting a reasonable delay for SPF computation can avoid occupying excessive device memory and bandwidth resources.

A smaller value set for *spf-delay* and *spf-holdtime* indicates that the OSPF can adapt to topology changes more quickly. In other words, a shorter network convergence time means that more CPU time of the router will be occupied.

The configurations of **timers spf** and **timers throttle spf** are mutually overwritten.

Examples

The following example configures the delay time for SPF computation after an OSPF process receives the topology change information as 3s and the time interval between two SPF computations as 9s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 20
Hostname(config-router)# timers spf 3 9
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1.86 timers throttle lsa all

Function

Run the **timers throttle lsa all** command to configure an exponential backoff algorithm of LSA packet generation.

Run the **no** form of this command to restore the default configuration.

By default, the minimum delay of LSA generation is 0 ms, the minimum interval between the first update and the second update of LSA is 5,000 ms, and the maximum interval between consecutive LSA updates is 5,000 ms.

Syntax

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

delay-time: Minimum delay for LSA generation, in milliseconds. The first LSA in the database is always generated instantly. The value range is from 0 to 600000.

hold-time: Minimum interval between the first LSA update and the second LSA update, in milliseconds. The value range is from 1 to 600000.

max-wait-time: Maximum interval between two LSA updates when the LSA is updated continuously, in milliseconds. This interval is also used to determine whether the LSA is updated continuously. The value range is from 1 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a high convergence requirement is raised when a link changes, you can set *delay-time* to a smaller value. To reduce the CPU usage, you can set *delay-time, hold-time* and *max-wait-time* to larger values.

When this command is configured, the value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.

Examples

The following example configures the first delay as 10 ms, the minimum interval between the first update and the second update of LSA as 1s, and the maximum interval between two LSA updates as 5s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# timers throttle lsa all 10 1000 5000
```

Notifications

When the configured value of *max-wait-time* is smaller than that of *hold-time*, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

When the configured value of *hold-time* is smaller than that of *delay-time*, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

The configured value of *hold-time* is smaller than that of *delay-time*, or the configured value of *max-wait-time* is smaller than that of *hold-time*.

Platform Description

N/A

Related Commands

- **show ip ospf**

1.87 timers throttle route

Function

Run the **timers throttle route** command to configure the delay time for route computation when an OSPF process receives changed inter-area and external LSAs.

Run the **no** form of this command to restore the default configuration.

By default, the waiting time for inter-area route computation is 0 ms, and that of external route computation is 0 ms.

Syntax

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

inter-area: Indicates inter-area route computation.

ia-delay: Delay for inter-area route computation, in milliseconds. When an inter-area LSA change is detected, the route computation triggered by the OSPF process is performed at least after the delay for inter-area route computation elapses. The value range is from 0 to 600000.

ase: Indicates the external route computation.

ase-delay: Delay for external route computation, in milliseconds. When an external LSA change is detected, the route computation triggered by the OSPF process is performed at least after the delay for external route computation elapses. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a strict requirement is raised for the network convergence time, use the default value. If a lot of inter-area or external routes exist on the network and the network is not stable, adjust the corresponding delays and optimize route computation to reduce the load on the device.

Examples

The following example configures the delay time for route computation when an OSPF process receives changed inter-area and external LSAs as 1s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# timers throttle route inter-area 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.88 timers throttle spf

Function

Run the **timers throttle spf** command to configure the delay time for SPF computation, and the minimum interval and maximum interval for two SPF computations after an OSPF process receives the topology change information.

Run the **no** form of this command to restore the default configuration.

By default, the delay for SPF computation is 1000 ms, the minimum interval for two SPF computations is 5000 ms, and the maximum interval between two SPF computations is 10,000 ms.

Syntax

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

spf-delay: Delay for SPF computation, in milliseconds. When a topology change is detected, the SPF computation triggered by the OSPF process is performed at least after the delay for SPF computation elapses. The value range is from 1 to 600000.

spf-holdtime: Minimum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

spf-max-waittime: Maximum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Here, *spf-delay* indicates the minimum time between the occurrence of a topology change and the start of SPF computation. The minimum interval between the first SPF computation and the second SPF computation is *spf-holdtime*. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches *spf-max-waittime*, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval for SPF computation is calculated starting from *spf-holdtime*.

You can set *spf-delay* and *spf-holdtime* to smaller values to accelerate topology convergence. Set *spf-max-waittime* to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology.

Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to run the **timers throttle spf** command for configuration.

- The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, *spf-holdtime* will be automatically set to the value of *spf-delay*.
- The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
- The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
- When neither **timers spf** nor **timers throttle spf** is configured, the default value of **timers throttle spf** prevails.

Examples

The following example configures the SPF computation delay, minimum interval and maximum interval of an OSPF process as 5 ms, 1,000 ms, and 90,000 ms in turn. If the topology changes continuously, the SPF computation time is as follows: 5 ms, 1s, 3s, 7s, 15s, 31s, 63s, 89s, 179s, 179+90.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router ospf 20
Hostname(config-router)# timers throttle spf 5 1000 90000
```

Notifications

When the configured value of **max-wait-time** is smaller than that of **hold-time**, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

When the configured value of **hold-time** is smaller than that of **delay-time**, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

The configured value of *hold-time* is smaller than that of *delay-time* or the configured value of *max-wait-time* is smaller than that of *hold-time*.

Platform Description

N/A

Related Commands

- **show ip ospf**

1.89 two-way-maintain

Function

Run the **two-way-maintain** command to enable the two-way maintenance function of an OSPF process.

Run the **no** form of this command to disable the two-way maintenance function of an OSPF process.

By default, the two-way maintenance function is enabled for an OSPF process.

Syntax

two-way-maintain

no two-way-maintain

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

On a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a result, some packets are delayed or discarded. If the time required for processing hello packets exceeds the neighbor dead interval, the corresponding adjacency times out and is removed. If the two-way maintenance

function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded hello packets.

Examples

The following example enables the two-way maintenance function of an OSPF process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 1
Hostname(config-router)# no two-way-maintain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip ospf**

1 OSPFv3 Commands

Command	Function
area authentication	Enable OSPFv3 area authentication.
area default-cost	Configure the cost of the default route in a stub area or not-so-stubby area (NSSA) on the ABR that resides in the stub area or NSSA.
area encryption	Enable OSPFv3 area encryption and authentication.
area nssa	Configure an OSPFv3 area as NSSA.
area range	Configure a range of summarized inter-area routes.
area stub	Configure an area as a stub or totally stub area.
area virtual-link	Create a virtual link or set virtual link parameters.
asbr enable	Configure a device as an ASBR.
auto-cost reference-bandwidth	Enable metric computation or reference bandwidth value modification for an interface based on bandwidth.
bfd all-interfaces	Enable bidirectional forwarding detection (BFD) on all OSPFv3 interfaces for link detection.
clear ipv6 ospf process	Clear and reset an OSPFv3 process.
default-information originate	Generate a default route and inject the route to an OSPFv3 routing domain.
default-metric	Configure the default metric of a redistributed route.
distance	Configure the administrative distances corresponding to different types of OSPFv3 routes.
distribute-list in	Enable the function of filtering routes that are computed based on the received LSAs.
distribute-list out	Enable the function of filtering redistributed routes.
enable mib-binding	Bind an MIB to a specified OSPFv3 process.
enable traps	Enable sending of the specified trap message.
graceful-restart	Enable the OSPFv3 GR capability.

graceful-restart helper	Enable the OSPFv3 GR helper function and configure a topology detection method of the OSPFv3 GR helper.
ipv6 ospf area	Enable an interface to join in an OSPFv3 routing process.
ipv6 ospf authentication	Enable OSPFv3 authentication on an interface.
ipv6 ospf bfd	Enable BFD on a specified OSPFv3 interface for link detection.
ipv6 ospf cost	Configure cost of an interface.
ipv6 ospf dead-interval	Configure the neighbor dead interval of an interface.
ipv6 ospf encryption	Enable OSPFv3 encryption on an interface.
ipv6 ospf hello-interval	Configure the hello packet sending interval on an interface.
ipv6 ospf mtu-ignore	Disable MTU verification for an interface that receives database description packets.
ipv6 ospf neighbor	Configure OSPFv3 neighbors.
ipv6 ospf network	Configure an OSPF network type of an interface.
ipv6 ospf priority	Configure the priority of an interface.
ipv6 ospf retransmit-interval	Configure the LSA retransmission interval on an interface.
ipv6 ospf subvlan	Enable the OSPFv3 function in a super VLAN.
ipv6 ospf transmit-delay	Configure the LSU transmission delay on an interface.
ipv6 router ospf	Enable an OSPFv3 routing process.
ipv6 router ospf max-concurrent-dd	Configure the maximum number of neighbors with which all the OSPFv3 routing processes can concurrently initiate or accept interaction.
log-adj-changes	Record the log of adjacency state changes.
max-concurrent-dd	Configure the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction.
nsr	Enable the nonstop routing (NSR) function.
passive-interface	Configure a passive interface.

redistribute	Enable route redistribution and inject routing information of other routing protocols to an OSPFv3 routing process.
router-id	Configure the ID of a router.
show ipv6 ospf	Display information of an OSPFv3 process.
show ipv6 ospf database	Display the database information of an OSPFv3 process.
show ipv6 ospf interface	Display the information of an OSPFv3 interface.
show ipv6 ospf neighbor	Display neighbor information of an OSPFv3 process.
show ipv6 ospf restart	Display the information related to OSPFv3 GR.
show ipv6 ospf route	Display the routing information of OSPFv3.
show ipv6 ospf summary-prefix	Display external route summarization information of OSPFv3.
show ipv6 ospf topology	Display the topological information of an OSPFv3 area.
show ipv6 ospf virtual-links	Display virtual link information of an OSPFv3 process.
summary-prefix	Configure a summarized route for the external routes of an OSPFv3 routing domain.
timers lsa arrival	Configure the delay for receiving same LSAs.
timers pacing lsa-group	Configure a group update time of LSAs.
timers pacing lsa-transmit	Configure the LSA group sending interval.
timers spf	Configure the delay time for SPF computation after an OSPFv3 process receives the topological change information and the interval between two SPF computations.
timers throttle lsa all	Configure an exponential backoff algorithm of LSA packet generation.
timers throttle route	Configure the delay time for route computation when an OSPFv3 process receives changed inter-area and external LSAs.
timers throttle spf	Configure the delay time for SPF computation when an OSPFv3 process receives topological change information, and the minimum and maximum intervals for two SPF computations.

two-way-maintain	Enable the two-way maintenance function of OSPFv3.

1.1 area authentication

Function

Run the **area authentication** command to enable OSPFv3 area authentication.

Run the **no** form of this command to disable this function.

The OSPFv3 area authentication function is disabled by default.

Syntax

area *area-id* **authentication ipsec spi** *sip* { **md5** [**string-key**] | **sha1** } [**0** | **7**] *key*

no area *area-id* **authentication**

Parameter Description

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Enables the MD5 authentication mode.

string-key: Specifies to use a string as an authentication key.

sha1: Enables the SHA1 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Enabling authentication can improve interaction security of OSPFv3 packets. A device supports four types of authentication:

- No authentication (when authentication is not configured)
- MD5
- SHA1

After an OSPFv3 area is configured with authentication, the configuration takes effect on all interfaces (except virtual links) in the area. If the interface authentication configuration is different from area authentication configuration, interface authentication configuration takes precedence over the area authentication configuration.

OSPFv3 area authentication and area associated SA authentication are mutually exclusive.

Examples

The following example configures MD5 for Area 1 in the OSPFv3 routing process, and sets the security parameter index to 300 and the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

The following example configures MD5 for Area 0 in the OSPFv3 routing process, and sets the security parameter index to 606 and the key to psw@123.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Hostname(config-router)# area 0 authentication ipsec spi 606 md5 string-key psw@123
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured in the local area, the following notification will be displayed:

```
% OSPFv3: Area is already configured with the same SPI.
```

If authentication is configured for an area with encryption configuration, the following notification will be displayed:

```
% OSPFv3: Area is already configured with encryption so cannot configure
authentication.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.2 area default-cost

Function

Run the **area default-cost** command to configure the cost of the default route in a stub area or not-so-stubby area (NSSA) on the ABR that resides in the stub area or NSSA.

Run the **no** form of this command to restore the default configuration.

The default cost value of the default route is **1**.

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

area-id: ID of a stub area or an NSSA, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

cost: Cost of the default summarized route injected to the stub area or NSSA. The value range is from 0 to 16777215.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The ABR in the stub area or NSSA will advertise the default route to the devices in the area. The default cost value of the default route is **1**. To lower the routing priority of the default route, you can use this command to set the cost to a greater value.

Examples

The following example sets the cost of the default route in a stub area to 100 on the ABR that resides in the stub area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 50 stub
Hostname(config-router)# area 50 default-cost 100
```

Notifications

When this command is configured in the backbone area, the following notification will be displayed:

```
% You can't configure default-cost to backbone
```

When this command is configured in a non-stub area or non-NSSA, the following notification will be displayed:

```
% The area is neither stub, nor NSSA
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.3 area encryption

Function

Run the **area encryption** command to enable OSPFv3 area encryption and authentication.

Run the **no** form of this command to disable this function.

The encryption and authentication function is disabled by default.

Syntax

area *area-id* **encryption ipsec spi** *spi* **esp** { { **3des** | **aes-cbc** { **128** | **192** | **256** } | **des** } [**0** | **7**] *des-key* | **null** } { **md5** | **sha1** } [**0** | **7**] *key*

no area *area-id* **encryption**

Parameter Description

Area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

esp: Enables the ESP encryption mode.

3des: Enables the 3DES encryption mode.

aes-cbc [**128** | **192** | **256**]: Enables the Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) encryption mode. The encryption key length is 128, 192, or 256 bits.

des: Enables the Data Encryption Standard (DES) mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

null: Indicates that no encryption mode is used.

md5: Enables the MD5 authentication mode.

sha1: Enables the SHA1 authentication mode.

key: Authentication key.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Enabling encryption and authentication can improve interaction security of OSPFv3 packets. A device supports the following types of encryption and authentication:

- Encryption modes: DES, 3DES, and AES-CBC.
- Authentication modes: MD5 and SHA1

After an OSPFv3 area is configured with encryption and authentication, the configuration takes effect on all interfaces (except virtual links) in the area, but the interface encryption and authentication configuration takes precedence over the area configuration.

Examples

The following example enables the OSPFv3 encryption and authentication function for Area 1, configures Area 1 with null encryption and MD5 authentication, and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured in the local area, the following notification will be displayed:

```
% OSPFv3: Area is already configured with the same SPI.
```

If encryption and authentication is re-configured for an area with authentication configuration, the following notification will be displayed:

```
% OSPFv3: Area is already configured with authentication so cannot configure
encryption.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.4 area nssa

Function

Run the **area nssa** command to configure an OSPFv3 area as NSSA.

Run the **no** form of this command to remove this configuration.

The NSSA function is disabled by default.

Syntax

area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** ***stability-interval***] *] *

no area *area-id* **nssa** [**default-information-originate** [**metric** | **metric-type**] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval**] *] *

Parameter Description

area-id: ID of the NSSA, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

default-information-originate: Indicates that generated default Type 7 LSAs are introduced to the NSSA. This option takes effect only on an NSSA ABR or ASBR.

metric *metric*: Indicates the metric of the generated default LSA. The value range is from 0 to 16777214, and the default value is **1**.

metric-type *metric-type*: Indicates the route type of the generated default LSA. *metric-type*: The value is **1** or **2**: **1** represents N-1, and **2** represents N-2. The default value is **2**.

no-redistribution: Select this option if the router is an NSSA ABR and you want to use the **redistribute** command to introduce the routing information only to a common area instead of an NSSA.

no-summary: Prohibits the ABR in the NSSA from sending Summary LSAs (Type 3 LSAs).

translator: Configures an ABR translator in an NSSA.

always: Enables the current NSSA ABR to always act as a translator. The default value is the standby translator.

stability-interval *stability-interval*: Configures the stability interval after the NSSA ABR is changed from a translator to a non-translator, in seconds. The value range is from 0 to 2147483647, and the default value is **40**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If you expect to reduce the LSA number in an area and to redistribute external routes, you can configure this area as an NSSA.

Parameter configurations are used as follows:

- The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table.
- If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be distributed to the NSSA. This parameter is generally used when a router in the NSSA acts both as an ASBR and an ABR. It prevents external routing information from entering the NSSA.

- The **no-summary** parameter is used to further reduce the number of LSAs sent to the NSSA and prevent the ABR from sending Summary LSAs (Type 3 LSAs) to the NSSA.
- The **area default-cost** parameter is used on an ABR/ASBR in this NSSA. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA. The default cost of the default route sent to the NSSA is 1.
- If an NSSA has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for translating Type 7 LSAs to Type 5 LSAs. If you expect that the current device is always the translator ABR for translating Type 7 LSAs to Type 5 LSAs, use the **translator always** parameter.
- If the translator role of the current device is replaced by another ABR, the translation capability of the device is retained during the time specified by **stability-interval**. If the device does not become a translator again during the time, LSAs that are translated from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires.
- To prevent a routing loop, LSAs that are translated from Type 7 to Type 5 are deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire.
- In the same NSSA, it is recommended that **translator always** be configured on only one ABR.

Examples

The following example configures OSPFv3 Area 1 as an NSSA.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 nssa
```

Notifications

If the backbone area is configured as an NSSA, the following notification will be displayed:

```
% You can't configure NSSA to backbone
```

If a stub area is configured as an NSSA, the following notification will be displayed:

```
% The area is configured as stub area already
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf**
- **ipv6 router ospf**

1.5 area range

Function

Run the **area range** command to configure a range of summarized inter-area routes.

Run the **no** form of this command to remove this configuration or restore the default configuration.

Inter-area route summarization is not performed by default.

Syntax

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**]

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

Parameter Description

area-id: ID of the OSPF area to which the summarized routes will be injected, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

ipv6-prefix/prefix-length: Range of IP addresses to be summarized.

advertise: Advertises the range of summarized routes.

not-advertise: Does not advertise the range of summarized routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only on an ABR, and is used to summarize multiple routes in an area as a route and advertise this route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. You can configure **advertise** or **not-advertise** to determine whether to advertise the range of summarized routes, which helps shield and filter routes. By default, the summarized routes are advertised.

You can configure the route summarization command for multiple areas to simplify the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network.

When multiple summarized routes are configured and have an inclusive relationship with each other, the range of routes to be summarized is determined based on the longest match principle.

Examples

The following example sets the IP address of the inter-area route summarization in Area 1 to 2001:DB8:1:2::/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 range 2001:db8:1:2::/64
```

Notifications

If an inexistent summarization entry is deleted, the following notification will be displayed:

```
% Can't find specified area range.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.6 area stub

Function

Run the **area stub** command to configure an area as a stub or totally stub area.

Run the **no** form of this command to remove this configuration or restore the default configuration.

The stub area function is disabled by default.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

area-id: ID of a stub area, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

no-summary: This option is valid only on the ABR in a stub area. If this option is specified, the ABR only advertises one Type 3 LSA indicating the default route to the stub area, and does not advertise other Type 3 LSAs.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in the stub area. Devices in a stub area cannot learn external routes (Type 5 LSAs) of the AS. In actual application, external routes take up a large proportion of the LSDB. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol.

By default, an ABR in a stub area will generate a Type 3 LSA indicating the default fault and advertise the LSA to the stub area. In this way, devices in the stub area can access devices outside the AS.

To configure a totally stub area, add the **no-summary** keyword when you are running the **area stub** command on the ABR.

Examples

The following example creates a stub area 10 and enables the ABRs in stub area 10 to advertise only default routes to the stub area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 10 stub
Hostname(config-router)# area 10 stub no-summary
```

Notifications

If the backbone area is configured as a stub area, the following notification will be displayed:

```
% You can't configure stub to backbone
```

If an NSSA is configured as a stub area, the following notification will be displayed:

```
% The area is configured as NSSA area already
```

If a stub area is configured with a virtual link, the following notification will be displayed, indicating that the virtual link must be deleted to validate the configuration:

```
% First deconfigure all virtual link through this area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf**
- **ipv6 router ospf**

1.7 area virtual-link

Function

Run the **area virtual-link** command to create a virtual link or set virtual link parameters.

Run the **no** form of this command to remove this configuration or restore the default configuration.

No virtual link is configured by default.

Syntax

area *area-id* **virtual-link** *router-id* [**dead-interval** *dead-interval* | **hello-interval** *hello-interval* | **instance** *instance-id* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication ipsec spi** *spi* { **md5** | **sha1** } [**0** | **7**] *key* | **encryption ipsec spi** *spi* **esp** [**3des** | **aes-cbc** { **128** | **192** | **256** } [**0** | **7**] *des-key* | **des** [**0** | **7**] *des-key* | **null**] { **md5** | **sha1** } [**0** | **7**] *key*]

no area *area-id* **virtual-link** *router-id* [**dead-interval** | **hello-interval** | **instance** | **retransmit-interval** | **transmit-delay**] * [**authentication** | **encryption**]

Parameter Description

area-id: ID of an area where a virtual link exists, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

router-id: ID of a neighboring router of the virtual link.

dead-interval *dead-interval*: Indicates the time that the local interface of the virtual link detects the failure of the neighbor, in seconds. The value range is from 0 to 2147483647, and the default value is **40**.

hello-interval *hello-interval*: Indicates the time consumed to send a Hello packet on the local interface of the virtual link, in seconds. The value range is from 1 to 65535, and the default value is **10**.

instance *instance-id*: Specifies the instance of a virtual link. The value range is from 0 to 255.

retransmit-interval *retransmit-interval*: Indicates the retransmission time of an LSA on the local interface of the virtual link, in seconds. The value range is from 0 to 65535, and the default value is **5**.

transmit-delay *transmit-delay*: Indicates the delay after which the LSA is sent on the local interface of the virtual link, in seconds. The value range is from 0 to 65535, and the default value is **1**.

authentication ipsec spi *spi* { **md5** | **sha1** | **sha2-256** } [**0** | **7**] *key*: Defines OSPFv3 authentication.

Note

Authentication between neighbors must be consistent. The **service password-encryption** command enables a configured key to be displayed in ciphertext mode.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Specifies the MD5 authentication mode.

sha1: Specifies the SHA1 authentication mode.

sha2-256: Specifies the sha2-256 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

encryption ipsec spi *spi* **esp** [**3des** | **aes-cbc** { **128** | **192** | **256** } [**0** | **7**] *des-key* | **des** [**0** | **7**] *des-key* | **null**] { **md5** | **sha1** } [**0** | **7**] *key*: Defines OSPFv3 encryption and authentication.

Note

Encryption and authentication between neighbors must be consistent. The **service password-encryption** command enables a configured key to be displayed in ciphertext mode.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

3des: Specifies the 3DES encryption mode.

aes-cbc 128: Specifies 128-bit AES-CBC authentication mode.

aes-cbc 192: Specifies 192-bit AES-CBC authentication mode.

aes-cbc 256: Specifies 256-bit AES-CBC authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

des: Specifies the DES encryption mode.

null: Indicates that no encryption mode is used.

md5: Specifies the MD5 authentication mode.

sha1: Specifies the SHA1 authentication mode.

key: Authentication key.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

In an OSPFv3 AS, all areas must be connected to the backbone area to properly learn the routing information of the entire OSPFv3 AS. If an area cannot be directly connected to the backbone area, the virtual link can be used to connect this area to the backbone area.

The area where the virtual link is located cannot be a stub area or NSSA.

The **hello-interval**, **dead-interval**, and **instance** parameters configured for neighbors connected by a virtual link must be consistent; otherwise, the adjacency cannot be set up properly.

Examples

The following example creates a virtual link and sets the router ID of the virtual link to 192.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 virtual-link 192.1.1.1
```

Notifications

If a virtual link is configured in the backbone area, the following notification will be displayed:

```
% You can't configure virtual-link transit to backbone
```

If a virtual link is configured in a stub area or an NSSA, the following notification will be displayed:

```
% Area is a stub or NSSA so virtual links are not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf virtual-links

1.8 asbr enable

Function

Run the **asbr enable** command to configure a device as an ASBR.

Run the **no** form of this command to restore the default configuration.

No device is an ASBR by default.

Syntax

asbr enable

no asbr enable

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

After the **redistribute** or **default-information** command is executed, an OSPF router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, run the **asbr enable** command. If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command configuration remains valid, the device is still an ASBR.

Examples

The following example configures a device as an ASBR.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# asbr enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf database**

1.9 auto-cost reference-bandwidth

Function

Run the **auto-cost reference-bandwidth** command to enable metric computation or reference bandwidth value modification for an interface based on bandwidth.

Run the **no** form of this command to disable this function or restore the default configuration.

The default reference bandwidth value computed based on the metric of an interface is **100** Mbps.

Syntax

auto-cost reference-bandwidth *ref-bw*

no auto-cost reference-bandwidth

Parameter Description

reference-bandwidth *reference-bandwidth*: Specifies the reference bandwidth value, in Kbps. The value range is from 1 to 4294967.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The cost value of an OSPFv3 interface is equal to the reference bandwidth value/interface bandwidth. To enable OSPFv3 on a 100M link, it is recommended that the *ref-bw* value be adjusted to a greater value based on actual network bandwidth. For a 1000M network, the reference bandwidth value can be set to a value greater than 1000; for a 10G network, the reference bandwidth value can be set to a value greater than 10000.

You can run the **ipv6 ospf cost** command in interface configuration mode to specify the cost of the specified interface. The priority of this cost is higher than that of the metric computed based on the reference bandwidth value.

Examples

The following example sets the reference bandwidth value to 10 Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# auto-cost reference-bandwidth 10
```

Notifications

If the reference bandwidth value is modified, the following notification will be displayed:

```
% OSPFv3: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf interface**

1.10 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to enable bidirectional forwarding detection (BFD) on all OSPFv3 interfaces for link detection.

Run the **no** form of this command to restore the default configuration.

The BFD function is disabled on all interfaces by default.

Syntax

bfd all-interfaces

no bfd all-interfaces

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, OSPFv3 establishes a BFD session with a neighbor in the full neighbor relationship. The neighbor state is detected using the BFD mechanism. When the BFD neighbor fails, OSFPv3 immediately performs network convergence.

You can also run the **ipv6 ospf bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the configuration made using the **bfd all-interfaces** command in process configuration mode.

Examples

The following example enables BFD on all OSPFv3 interfaces for link detection.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# bfd all-interfaces
```

Notifications

If BFD is enabled on all interfaces for link detection, the following notification will be displayed:

```
% Warning: The BFD for OSPFv3 neighbor shall be enabled, or it would affect the route
learning.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.11 clear ipv6 ospf process

Function

Run the **clear ipv6 ospf process** command to clear and reset an OSPFv3 process.

Syntax

clear ipv6 ospf [*process-id*] **process**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535. When this parameter is specified, the specified OSPF process will be cleared and reset. When this parameter is not specified, all the running OSPF processes will be cleared and reset.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Resetting the whole OSPFv3 process will reestablish all the neighbors, which has a great impact on the entire protocol.

When running this command, you need to make confirmation.

Use the *process-id* parameter to specify to clear an OSPFv3 instance. If the *process-id* parameter is not specified, all OSPFv3 instances are cleared.

Examples

The following example clears and resets an OSPFv3 instance.

```
Hostname> enable
Hostname# clear ipv6 ospf process
```

Notifications

If the specified process ID is incorrect, the following notification will be displayed:

```
% OSPFv3: No router process 1.
```

Platform Description

N/A

Related Commands

N/A

1.12 default-information originate

Function

Run the **default-information originate** command to generate a default route and inject the route to an OSPFv3 routing domain.

Run the **no** form of this command to remove this configuration or restore the default configuration.

No default route is generated by default.

Syntax

default-information originate [**always** | **metric** *metric* | **metric-type** *type* | **route-map** *map*] *

no default-information originate [**always** | **metric** | **metric-type** | **route-map** *map*] *

Parameter Description

always: Enables OSPFv3 to generate a default route even if a default route exists locally.

metric *metric*: Indicates the initial metric of the default route. The value range is from 0 to 16777214, and the default value is **1**.

metric-type type: Indicates the type of the default route. The value is 1 or 2, and the default value is **2**.

route-map *map*: Indicates the name of the associated route map. No route map is associated by default.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the **redistribute** or **default-information** command is executed, an OSPFv3 router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all

routers in the OSPF routing domain. To enable an ASBR to generate a default route, run the **default-information originate** command.

If the **always** parameter is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf database** command to display the OSPFv3 LSDB. On an OSPFv3 neighbor, you can run the **show ipv6 route** command to display the default route.

The metric of the external default route can be defined only by the **default-information originate** command, instead of the **default-metric** command.

OSPFv3 has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ipv6 route** command displays only the Type 1 route.

This command generates a default route of Type 5 LSA, which will not be flooded to an NSSA. If you want to generate a default route in the NSSA, use the **area nssa default-information-originate** command. A router in the stub area cannot generate an external default route.

Examples

The following example generates a default route and injects the route to an OSPFv3 routing domain.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# default-information originate always
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf database**

1.13 default-metric

Function

Run the **default-metric** command to configure the default metric of a redistributed route.

Run the **no** form of this command to restore the default configuration.

The default metric of a redistributed route is **20**.

Syntax

default-metric *metric-value*

no default-metric

Parameter Description

metric-value: Default metric of a redistributed route. The value range is from 1 to 16777214.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used with the **redistribute** command to configure the default metric of a redistributed route. This command does not take effect to two types of routes:

- Default route generated by the **default-information originate** command.
- Redistributed direct route. The default metric of a redistributed direct route is always **20**.

Examples

The following example sets the default metric of a redistributed route to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# default-metric 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.14 distance

Function

Run the **distance** command to configure the administrative distances corresponding to different types of OSPFv3 routes.

Run the **no** form of this command to restore the default configuration.

The default administrative distance is **110** for all the OSPF routes.

Syntax

distance { *distance* | **ospf** { **external** *distance* | **inter-area** *distance* | **intra-area** *distance* } * }

no distance [**ospf**]

Parameter Description

distance: Administrative distance of a route. The value range is from 1 to 255.

distance: Configures an administrative distance of OSPFv3.

external *distance*: Indicates the administrative distance of an external route. The value range is from 1 to 255.

inter-area *distance*: Indicates the administrative distance of an inter-area route. The value range is from 1 to 255.

intra-area *distance*: Indicates the administrative distance of an internal route. The value range is from 1 to 255.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To compare the priorities of routes generated by different OSPF processes, use this command to specify the administrative distances corresponding to different types of OSPF routes.

The administrative distances of routes allow different routing protocols to compare route priorities. A smaller administrative distance indicates a higher route priority.

If the administrative distance of a route entry is set to 255, the route entry is not trustworthy and does not participate in packet forwarding.

Examples

The following example sets the administrative distance of an OSPFv3 external route to **160**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# distance ospf external 160
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.15 distribute-list in

Function

Run the **distribute-list in** command to enable the function of filtering routes that are computed based on the received LSAs.

Run the **no** form of this command to disable this function.

By default, the function of filtering routes computed based on the received LSAs is disabled, that is, all these routes get passed.

Syntax

distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

no distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*: Uses a prefix list for filtering.

interface-type interface-number: Type and number of an interface on which LSA routes are filtered.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command filters the routes that are computed based on received LSAs. Only the routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL and prefix list filtering rules are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes of a specified interface, prefix list cannot be configured for the same interface.

This command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Examples

The following example filters routes (that are computed based on the received LSAs) based on the prefix list aaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
Hostname(config)# ipv6 router ospf 25
Hostname(config-router)# redistribute rip metric 100
Hostname(config-router)# distribute-list prefix-list aaa in gigabitethernet 0/1
```

Notifications

If the configured interface is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

If the configured ACL name is invalid, the following notification will be displayed:

```
% ACL name abc-acl is invalid
```

If routes imported by this instance are filtered, the following notification will be displayed:

```
% Distribute-list of "ospf 1" via "ospf 1" not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.16 distribute-list out

Function

Run the **distribute-list out** command to enable the function of filtering redistributed routes.

Run the **no** form of this command to disable this function.

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes pass the filtering rules.

Syntax

distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list prefix-*list-name*: Uses a prefix list for filtering.

bgp: Filters BGP routes.

connected: Filters direct routes.

isis [*area-tag*]: Filters IS-IS routes.

ospf *process-id*: Filters OSPF routes.

rip: Filters RIP routes.

static: Filters static routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

As with the **redistribute route-map** command, the **distribute-list out** command filters routes that are redistributed from other protocols to OSPFv3. The **distribute-list out** command does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and prefix list are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes of a source, prefix list cannot be configured for the same source.

Examples

The following example filters redistributed static routes based on the prefix list jjj.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# redistribute static
Hostname(config-router)# distribute-list prefix-list jjj out static
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.17 enable mib-binding

Function

Run the **enable mib-binding** command to bind an MIB to a specified OSPFv3 process.

Run the **no** form of this command to restore the default configuration.

The MIB is bound to the OSPFv3 process with the minimum process ID by default.

Syntax

enable mib-binding

no enable mib-binding

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 MIB does not contain OSPFv3 process information. Therefore, SNMP operations take effect on one OSPFv3 process only.

If you wish to perform operations on a specified OSPFv3 process through SNMP, run this command to bind the MIB with the process.

Examples

The following example binds an MIB to a specified OSPFv3 process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 100
Hostname(config-router)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.18 enable traps

Function

Run the **enable traps** command to enable sending of the specified trap message.

Run the **no** form of this command to disable this function.

The trap function is disabled by default.

Syntax

enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] * | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** |

VirtNbrStateChange | **RestartStatusChange** | **NbrRestartHelperStatusChange** | **VirtNbrRestartHelperStatusChange**] *]

no enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] * | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange** | **RestartStatusChange** | **NbrRestartHelperStatusChange** | **VirtNbrRestartHelperStatusChange**] *]

Parameter Description

error: Configures all the trap switches related to Error. This parameter can also configure the following specific error trap switches:

IfConfigError: Indicates interface parameter configuration error.

IfRxBadPacket: Indicates that the interface receives an error packet.

VirtIfConfigError: Indicates virtual interface parameter configuration error.

VirtIfRxBadPacket: Indicates that the virtual interface receives an error packet.

state-change: Configures all the trap switches related to State-change. This parameter can also configure the following specific state-change trap switches:

IfStateChange: Indicates that the interface state changes.

NbrStateChange: Indicates that the neighbor state changes.

NssaTranslatorStatusChange: Indicates that the NSSA translator state changes.

VirtIfStateChange: Indicates that the virtual interface state changes.

VirtNbrStateChange: Indicates that the virtual neighbor state changes.

RestartStatusChange: Indicates that the local GR state changes.

NbrRestartHelperStatusChange: Indicates that the neighbor GR process state changes.

VirtNbrRestartHelperStatusChange: Indicates that the status of the virtual neighbor GR process changes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The function of this command is restricted by the **snmp-server** command. The **snmp-server enable traps ospf** command must be run prior to the **enable traps** command so that OSPFv3 Trap messages can be sent correctly.

This command is not restricted by the MIB bound to the process. The trap switch can be enabled concurrently for different processes.

Examples

The following example enables sending of the specified trap message.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 router ospf 100
Hostname(config-router)# enable traps
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **snmp-server enable traps ospf** (network management and monitoring/SNMP)

1.19 graceful-restart

Function

Run the **graceful-restart** command to enable the OSPFv3 GR capability.

Run the **no** form of this command to disable this function or restore the default configuration.

The OSPFv3 GR function is enabled by default.

Syntax

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [**grace-period** | **inconsistent-lsa-checking**]

Parameter Description

grace-period *grace-period*: Configures the GR time (in seconds), which starts at the time when OSPFv3 fails and ends at the time when OSPFv3 is restarted and GR is completed. The value range is from 1 to 1800, and the default value is **120**.

inconsistent-lsa-checking: Enables topology change detection. If any topology change is detected, OSPF exits the GR process to complete convergence.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When a GR-enabled router is restarted on the control plane, data forwarding can be still guided on the forwarding plane. In addition, actions such as neighbor relationship re-forming and route computation performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

The GR function is based on OSPFv3 instance configuration, and different instances can be configured with different parameters based on actual situation.

This command is used to configure the GR restarter capability of a router. In the GR period, link state reestablishment enables OSPFv3 to restore to the original state. When a GR period expires, OSPFv3 exits the GR state and executes normal OSPFv3 operations.

Run the **graceful-restart** command to set the GR period to 120s. The **graceful-restart grace-period** command allows you to modify the GR period explicitly.

If the Fast Hello function is enabled, the GR function cannot be enabled.

The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. In case of a topology change, OSPFv3 converges as soon as possible and does not wait for GR execution to avoid longtime forwarding black-hole.

- Disabling topology detection: If OSPFv3 cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time.
- Enabling topology detection: Forwarding interruption may occur, but the interruption time is far less than the forwarding black-hole time when topology detection is disabled.

In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process.

Examples

The following example enables the OSPFv3 restarter capability and sets the GR period to **60** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# graceful-restart
Hostname(config-router)# graceful-restart grace-period 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.20 graceful-restart helper

Function

Run the **graceful-restart helper** command to enable the OSPFv3 GR helper function and configure a topology detection method of the OSPFv3 GR helper.

Run the **no** form of this command to disable this function and remove this configuration.

The GR helper capability is enabled by default. After the GR helper is enabled on the device, LSA changes are not checked.

Syntax

graceful-restart helper { **disable** | **internal-lsa-checking** | **strict-lsa-checking** }

no graceful-restart helper { **disable** | **internal-lsa-checking** | **strict-lsa-checking** }

Parameter Description

disable: Disables a device to act as a GR helper for other devices.

internal-lsa-checking: Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

strict-lsa-checking: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the GR help capability of a device. When a device performs GR, it sends a Grace-LSA to notify all its neighbor devices. If the GR help capability is enabled on the local device, the local device becomes a GR helper upon receiving the Grace-LSA to help the former device complete GR. The **disable** option indicates that the GR helper is not provided for any device that implements GR.

After a device becomes a GR helper, the network changes are not detected by default. If any change takes place in the network, the network topology converges after GR is completed. If you expect that network change can be detected quickly during GR, configure the **strict-lsa-checking** or **internal-lsa-checking** option to enable detection. The former option detects any LSA (Type 1 to Type 5 and Type 7 LSAs) that indicates network information, and the latter option detects any LSA (Type 1 to Type 3 LSAs) that indicates routes in an AS domain. When the network scale is large, it is recommended that you disable the LSA checking options because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Examples

The following example disables the OSPFv3 GR helper function and configures the topology detection method as **strict-lsa-checking**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# graceful-restart helper disable
Hostname(config-router)# no graceful-restart helper disable
Hostname(config-router)# graceful-restart helper strict-lsa-checking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.21 ipv6 ospf area

Function

Run the **ipv6 ospf area** command to enable an interface to join in an OSPFv3 routing process.

Run the **no** form of this command to disable this function.

No interface joins in an OSPFv3 routing process by default.

Syntax

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area *area-id*: Specifies an OSPFv3 area that an interface joins in. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Run this command in interface configuration mode to enable an interface to join in OSPFv3, and then run the **ipv6 router ospf** command to configure an OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically join in the process. The adjacency can be set up only between devices with the same *instance ID*. After this command is configured, all prefix information on the interface will be used to participate in the OSPFv3 process.

The following methods can be used to disable an interface from joining in an OSPFv3 process.

- Run the **no** form of this command to disable an interface from joining an OSPFv3 process.
- Run the **no ipv6 router ospf** command to disable all interfaces from joining in an OSPFv3 process.

Examples

The following example enables an OSPFv3 process on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1))# ipv6 ospf 1 area 2 instance 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.22 ipv6 ospf authentication

Function

Run the **ipv6 ospf authentication** command to enable OSPFv3 authentication on an interface.

Run the **no** form of this command to disable this function.

By default, no authentication mode is configured on an interface. In this case, the authentication type of the area where the interface resides is used on the interface.

Syntax

ipv6 ospf authentication { **ipsec spi** *spi* { **md5** [**string-key**] | **sha1** } [**0** | **7**] *key* | **null** } [**instance** *instance-id*]

no ipv6 ospf authentication [**instance** *instance-id*]

Parameter Description

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Enables the MD5 authentication mode.

string-key: Specifies to use a string as an authentication key.

sha1: Enables the SHA1 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

null: Indicates that no authentication mode is enabled.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Use this command to enable OSPFv3 authentication on an interface.

The device supports four authentication types:

- No authentication (when authentication is not configured)
- MD5
- SHA1

After an OSPFv3 area is configured with authentication, the configuration takes effect on all interfaces (except virtual links) in the area. If the interface authentication configuration is different from area authentication configuration, interface authentication configuration takes precedence over the area authentication configuration.

OSPFv3 interface authentication and interface associated SA authentication are mutually exclusive.

Note

OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Examples

The following example configures an OSPFv3 interface with MD5 authentication mode and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured on the local Interface, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with the same SPI.
```

If authentication is configured on an interface with encryption configuration, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with encryption so cannot configure
authentication.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ipv6 ospf bfd

Function

Run the **ipv6 ospf bfd** command to enable BFD on a specified OSPFv3 interface for link detection.

Run the **no** form of this command to disable this function.

The BFD function is disabled on an interface by default, and the BFD configuration is subject to the configuration in the OSFPv3 process configuration mode.

Syntax

ipv6 ospf bfd [**disable**] [**instance** *instance-id*]

no ipv6 ospf bfd [**instance** *instance-id*]

Parameter Description

disable: Disables BFD on a specified OSPF interface for link detection.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Once a link is faulty, OSPF can quickly detect the failure of the route. This configuration helps shorten the traffic interruption time.

The BFD priority configured on an interface takes precedence over that configured in process configuration mode.

In light of the actual environment, you can run the **ipv6 ospf bfd** command to enable BFD on a specified OSPF interface for link detection, or run the **bfd all-interfaces** command in OSPFv3 process configuration mode to enable BFD on all OSPFv3 interfaces for link detection. Run the **ipv6 ospf bfd disable** command to disable BFD on a specified OSPF interface for link detection.

Examples

The following example enables BFD for link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf bfd
```

Notifications

If BFD is enabled for link detection on an interface, the following notification will be displayed:

```
% Warning: The BFD for OSPFv3 neighbor shall be enabled, or it would affect the route
learning.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.24 ipv6 ospf cost

Function

Run the **ipv6 ospf cost** command to configure cost of an interface.

Run the **no** form of this command to restore the default configuration.

The default cost of an interface is the reference bandwidth value/Bandwidth (the default reference bandwidth value is 100 Mbps).

Syntax

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf *cost* [**instance** *instance-id*]

Parameter Description

cost: Cost of an OSPFv3 interface. The value range is from 0 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The default cost value of an OSPFv3 interface is 100 Mbps/Bandwidth. Bandwidth indicates the bandwidth of the interface and it is configured by running the **bandwidth** command in interface configuration mode.

The default interface costs of several typical OSPFv3 lines are as follows:

- For the 64 Kbps serial line, the cost is 1562.
- For the E1 line, the cost is 48.
- For the 10 Mbps Ethernet, the cost is 10.
- For the 100 Mbps Ethernet, the cost is 1.

The OSPFv3 cost configured through the **ipv6 ospf cost** command will overwrite the default configuration.

Examples

The following example sets the cost of an interface to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf cost 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.25 ipv6 ospf dead-interval

Function

Run the **ipv6 ospf dead-interval** command to configure the neighbor dead interval of an interface.

Run the **no** form of this command to restore the default configuration.

The fast hello function is disabled by default, and the neighbor dead interval is four times the sending interval of hello packets.

Syntax

ipv6 ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description

Dead-interval: Neighbor dead interval, in seconds. The value range is from 0 to 2147483647.

minimal hello-multiplier: Enables the fast hello function and sets the neighbor dead interval to **1** second.

multiplier: Hello packet sending times per second. The value range is from 3 to 20.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 neighbor dead interval is contained in hello packets. If OSPF does not receive a hello packet from a neighbor within the neighbor dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. By default, the neighbor dead interval is four times the hello packet sending interval. If the hello packet sending interval is modified, the neighbor dead interval is modified automatically.

This command can be used to manually modify the neighbor dead interval. However, the configuration must be made with caution. Pay attention to the following two issues:

(1) The dead interval cannot be smaller than the hello packet sending interval.

(2) The dead interval must be the same on all routers in the same network segment.

OSPFv3 supports the fast hello function:

Enabling the OSPFv3 fast hello function allows OSPFv3 to find neighbors more quickly and detect neighbor failures faster. You can enable the OSPFv3 fast hello function by specifying the **minimal hello-multiplier** keyword and the *multiplier* parameter. The **minimal** keyword sets the dead interval to 1s, and the value of **hello-multiplier** specifies the hello packet sending times per second. In this way, the hello packet sending interval drops to less than 1s.

If the fast hello function is enabled on an interface, the hello-interval field of the hello packets advertised on the interface is set to 0, and the hello-interval field of the hello packets received on this interface is ignored.

Note

The *dead-interval*, *minimal hello-multiplier*, and *hello-interval* parameters introduced for the fast hello function cannot be configured simultaneously.

No matter whether the fast hello function is enabled, the neighbor dead interval must be consistent among neighbor interfaces. The **hello-multiplier** value can be inconsistent provided that at least one hello packet can be received within the neighbor dead interval.

Run the **show ipv6 ospf interface** command to display the dead interval and fast hello interval configured for an interface.

Examples

The following example sets the neighbor dead interval of an interface to **60** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 60
```

Notifications

If the neighbor dead interval is smaller than the hello packet sending interval, the following notification will be displayed:

```
% Warning: OSPFv3 dead interval should be higher than hello interval
```

If the hello packet sending interval is configured prior to the fast hello function, the following notification will be displayed:

```
% OSPFv3: Hello interval configured with hello-interval.
```

Common Errors

- The neighbor dead intervals configured on different ports in the same area are inconsistent.

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.26 ipv6 ospf encryption

Function

Run the **ipv6 ospf encryption** command to enable OSPFv3 encryption on an interface.

Run the **no** form of this command to disable this function.

Encryption is disabled by default.

Syntax

ipv6 ospf encryption { **ipsec spi** *spi* **esp** { { **3des** | **aes-cbc** { **128** | **192** | **256** } | **des** } [**0** | **7**] *des-key* | **null** } { **md5** | **sha1** } [**0** | **7**] *key* | **null** } [**instance** *instance-id*]

no ipv6 ospf encryption [**instance** *instance-id*]

Parameter Description

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

esp: Enables the ESP encryption mode.

des: Enables the DES encryption mode.

3des: Enables the 3DES encryption mode.

aes-cbc [**128** | **192** | **256**]: Enables the Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) encryption mode. The encryption key length is 128, 192, or 256 bits.

des: Enables the DES encryption mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

null: Indicates that no encryption mode is used.

md5: Enables the MD5 authentication mode.

sha1: Enables the SHA1 authentication mode.

key: Authentication key.

null: Indicates that no authentication mode is enabled.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

The device supports the following types of encryption and authentication:

Encryption modes: DES, 3DES, and AES-CBC.

Authentication modes: MD5 and SHA1

Note

OSPFv3 encryption and authentication parameters configured on the interconnected interfaces must be consistent.

Examples

The following example enables OSPFv3 encryption and authentication for an interface, configures the interface with null encryption and MD5 authentication, and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured on the local Interface, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with the same SPI.
```

If encryption and authentication is re-configured for an interface with authentication configuration, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with authentication so cannot configure encryption.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.27 ipv6 ospf hello-interval

Function

Run the **ipv6 ospf hello-interval** command to configure the hello packet sending interval on an interface.

Run the **no** form of this command to restore the default configuration.

The default hello packet sending interval of the broadcast and P2P networks is **10** seconds. The default hello packet sending interval of the P2MP and NBMA networks is **30** seconds.

Syntax

ipv6 ospf hello-interval *hello-interval* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

hello-interval: Hello packet sending interval, in seconds. The value range is from 1 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The hello packet sending interval is contained in hello packets. A shorter interval indicates that OSPFv3 can detect topology changes more quickly, but the network traffic increases. The hello packet sending interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the hello packet sending interval.

Note

The *dead-interval minimal hello-multiplier* and *hello-interval* parameters introduced for the fast hello function cannot be configured simultaneously.

Examples

The following example sets the hello packet sending interval to **20** seconds on the interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 20
```

Notifications

If the hello packet sending interval is configured on an interface that is configured with the *dead-interval minimal hello-multiplier* parameter of the fast hello function, the following notification will be displayed:

```
% OSPFv3: Hello interval configured with hello-multiplier.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.28 ipv6 ospf mtu-ignore

Function

Run the **ipv6 ospf mtu-ignore** command to disable MTU verification for an interface that receives database description packets.

Run the **no** form of this command to enable MTU verification for an interface that receives database description packets.

The MTU verification function is disabled by default.

Syntax

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter Description

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

On receiving a database description packet, OSPFv3 checks whether the MTU of the neighbor interface in the database description packet is the same as the MTU of the local interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency fails to be set up. To resolve this problem, you can disable MTU verification.

Examples

The following example disables MTU verification for an interface that receives database description packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ipv6 ospf neighbor

Function

Run the **ipv6 ospf neighbor** command to configure OSPFv3 neighbors.

Run the **no** form of this command to restore the default configuration.

No neighbor is configured by default.

Syntax

ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *value*] *] [**instance** *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *value*] *] [**instance** *instance-id*]

Parameter Description

cost *cost*: Configures costs required to reach each neighbor in the P2MP network. This parameter is not defined by default and applicable only to the P2MP network. The value range is from 0 to 65535.

poll-interval *poll-interval*: Indicates the neighbor polling interval, in seconds. This parameter is applicable only to the NBMA network. The value range is from 0 to 2147483647, and the default value is **120**.

priority *priority*: Configures the priority of a neighbor in the NBMA network. This parameter is applicable only to the NBMA network. The value range is from 0 to 255, and the default value is **0**.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IPv6 address of an OSPFv3 neighbor to FE80::2D0:F8FF:FE22:3533, priority value to **1**, and polling interval to **150** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf network non-broadcast
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf neighbor fe80::2d0:f8ff:fe22:3533
priority 1 poll-interval 150
```

Notifications

If a neighbor is configured in the NBMA and P2MP networks, the following notification will be displayed:

```
% Neighbor command is allowed only on NBMA and point-to-multipoint networks.
```

If the IP address of a specified neighbor is not an IPv6 address, the following notification will be displayed:

```
% OSPFv3: Neighbor address needs to be a link-local address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 ipv6 ospf network

Function

Run the **ipv6 ospf network** command to configure an OSPF network type of an interface.

Run the **no** form of this command to restore the default configuration.

By default, the interface type of OSPF is not configured. No interface is set to P2MP type by default.

Syntax

ipv6 ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** } [**instance** *instance-id*]

no ipv6 ospf network [**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**] [**instance** *instance-id*]

Parameter Description

broadcast: Configures the broadcast network type for an interface.

non-broadcast: Configures the non-broadcast network type for an interface.

point-to-multipoint: Configures the P2MP network type for an interface.

point-to-multipoint non-broadcast: Configures the P2MP non-broadcast network type for an interface.

point-to-point: Configures the P2P network type for an interface.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

OSPFv3 network types are configured based on the network architecture. Ethernet and FDDI belong to the broadcast type. X.25, frame relay, and ATM belong to the NBMA type. PPP, HDLC, and LAPB belong to the P2P type. Each network type is restricted as follows:

- The broadcast type requires that the interfaces must have the broadcast capability.
- The P2P type requires that the interfaces are interconnected in one-to-one manner.
- The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.
- The P2MP type does not raise any requirement.

Examples

The following example configures the OSPF network type of an interface as P2P.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf network point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.31 ipv6 ospf priority

Function

Run the **ipv6 ospf priority** command to configure the priority of an interface.

Run the **no** form of this command to restore the default configuration.

The priority value is **1** by default.

Syntax

ipv6 ospf priority *priority* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description

priority: Priority of an interface. The value range is from 0 to 255.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In a broadcast network, a DR or BDR must be elected. During the DR or BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR.

A device with the priority 0 does not participate in the DR or BDR election.

Examples

The following example sets the priority of an interface to **0** so that the interface does not participate in the DR or BDR election.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.32 ipv6 ospf retransmit-interval

Function

Run the **ipv6 ospf retransmit-interval** command to configure the LSA retransmission interval on an interface.

Run the **no** form of this command to restore the default configuration.

The default LSA retransmission interval is **5** seconds.

Syntax

ipv6 ospf retransmit-interval *retransmit-interval* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter Description

retransmit-interval: LSU retransmission interval, in seconds. The value range is from 1 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To ensure transmission reliability of the routing information, a router must get confirmation from a neighbor when sending LSAs to the neighbor. Users can use this command to configure the interval of waiting for confirmation from a neighbor based on the actual running environment. If no confirmation is received within the specified interval, the router retransmits LSAs.

The LSU retransmission interval must be longer than the round-trip transmission delay of data packets between two neighbors.

Examples

The following example sets the LSA transmission interval on an interface to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf retransmit-interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.33 ipv6 ospf subvlan

Function

Run the **ipv6 ospf subvlan** command to enable the OSPFv3 function in a super VLAN.

Run the **no** form of this command to restore the default configuration.

The OSPFv3 function takes effect in super VLANs only and is disabled by default.

Syntax

ipv6 ospf subvlan [**all** | *vlan-id*]

no ipv6 ospf subvlan

Parameter Description

all: Allows sending packets to all sub VLANs.

vlan-id: Sub VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In normal cases, a super VLAN contains multiple sub VLANs. The multicast packets corresponding to a super VLAN are also sent to its sub VLANs. OSPFv3 multicast packets will be replicated when they are sent in a super VLAN. If the super VLAN contains many sub VLANs, a great number of OSPF multicast packets are replicated, exceeding the processing capability of the device. This results in discarding of many packets and causes protocol flapping.

In most scenarios, the OSPFv3 function does not need to be enabled in a super VLAN, and it is disabled by default. In some other scenarios, OSPFv3 needs to be run in a super VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. Usually, packets need to be sent to only one sub VLAN. You can run this command to specify a sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the OSPFv3 function on super VLAN 300 and allows sending packets to sub VLAN 1024.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# ipv6 ospf subvlan 1024
```

Notifications

N/A

Common Errors

- The function is configured on a non-super VLAN.
- The specified sub VLAN on the super VLAN cannot implement interworking with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.34 ipv6 ospf transmit-delay

Function

Run the **ipv6 ospf transmit-delay** command to configure the LSU transmission delay on an interface.

Run the **no** form of this command to restore the default configuration.

The LSU packet transmission time is **1** second by default.

Syntax

ipv6 ospf transmit-delay *transmit-delay* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter Description

transmit-delay: Delay for an OSPF interface to transmit LSU packets, in seconds. The value range is from 1 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The sending delay and line transmission delay of the interface must be considered when *transmit-delay* is configured. For a low-speed line, the transmission delay of the interface must be set to a value greater than the default value.

Examples

The following example sets the LSU transmission delay on an interface to **2** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf transmit-delay 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.35 ipv6 router ospf

Function

Run the **ipv6 router ospf** command to enable an OSPFv3 routing process.

Run the **no** form of this command to disable this process.

No OSPFv3 routing process is enabled by default.

Syntax

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

no ipv6 router ospf *process-id*

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535, and the default value is **1**.

vrf-name: VRF to which the OSPFv3 process belongs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Run this command to enable an OSPFv3 routing process, and the device enters the routing process configuration mode.

A maximum of 32 OSPFv3 processes can be configured.

Examples

The following example enables an OSPFv3 process in vrf:vpn_1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1 vrf vpn_1
```

Notifications

When an OSPFv3 process fails to be configured because **ipv6 unicast-routing** is not enabled, the following notification will be displayed:

```
IPv6 unicast-routing not enabled, OSPFv3 process can't configure
```

When the corresponding OSPFv3 process cannot be enabled because it is not allocated a router ID, the following notification will be displayed:

```
%OSPFV3-NORTRID: OSPFv3 process 1 failed to allocate unique router-id and cannot start.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf**

1.36 ipv6 router ospf max-concurrent-dd

Function

Run the **ipv6 router ospf max-concurrent-dd** command to configure the maximum number of neighbors with which all the OSPFv3 routing processes can concurrently initiate or accept interaction.

Run the **no** form of this command to restore the default configuration.

The maximum number of neighbors is **10** by default.

Syntax

ipv6 router ospf max-concurrent-dd *max-neighbor*

no ipv6 router ospf max-concurrent-dd

Parameter Description

max-neighbor: Maximum number of neighbors that concurrently interact with the OSPF process. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can run this command to restrict the maximum of neighbors with which all OSPFv3 processes can concurrently initiate or accept interaction.

Examples

The following example sets the maximum number of neighbors with which all OSPFv3 processes can concurrently initiate or accept interaction to **4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 log-adj-changes

Function

Run the **log-adj-changes** command to record the log of adjacency state changes.

Run the **no** form of this command to remove this configuration.

The log record function is enabled by default.

Syntax

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

detail: Displays detailed information of neighbor state changes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The log records the log information of the following four types of events only:

The adjacency reaches the full state;

The adjacency leaves the full state;

The adjacency reaches the down state;

The adjacency leaves the down state.

Examples

The following example records the log of adjacency state changes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# log-adj-changes detail
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.38 max-concurrent-dd

Function

Run the **max-concurrent-dd** command to configure the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction.

Run the **no** form of this command to restore the default configuration.

The maximum number of concurrent neighbors is **5** by default.

Syntax

max-concurrent-dd *neighbor-number*

no max-concurrent-dd

Parameter Description

neighbor- number: Maximum number of neighbors that concurrently interact with the OSPF instance. The value range is from 1 to 65535.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can run this command to restrict the maximum number of neighbors with which each OSPFv3 instance can concurrently initiate or accept interaction.

Examples

The following example sets the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction to **4**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.39 nsr

Function

Run the **nsr** command to enable the nonstop routing (NSR) function.

Run the **no** form of this command to restore the default configuration.

The NSR function is disabled by default.

Syntax

nsr

no nsr

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

During NSR, OSPFv3-related information is backed up from the active supervisor module of a distributed device to the standby supervisor module, or from the active host of a virtual switching unit (VSU) to the standby host. In this way, the device can automatically recover the link state and re-generate routes without the help of the neighbor devices during the active/standby switchover. Information that should be backed up includes the neighbor relationship and link state.

For the same OSPFv3 instance, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is supported.

The switchover of devices in distributed or VSU mode takes a period of time. If OSPFv3 neighbor keepalive duration is shorter than the switchover duration, the OSPFv3 neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, you are advised to set the OSPFv3 neighbor keepalive duration not less than the default value when you are enabling the NSR function. When fast hello is enabled, the OSPFv3 neighbor keepalive duration is less than 1s and the OSPFv3 neighbor relationship times out during the switchover, causing NSR failures. Therefore, you are advised to disable fast hello when NSR is enabled.

Examples

The following example enables the NSR function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# nsr
```

Notifications

N/A

Common Errors

- The neighbor keepalive duration is short. When fast hello is enabled, the OSPFv3 neighbor relationship is removed during a switchover, causing forwarding interruption.

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.40 passive-interface

Function

Run the **passive-interface** command to configure a passive interface.

Run the **no** form of this command to restore the default configuration.

The passive mode of interfaces is disabled by default, and all interfaces are allowed to send and receive OSPFv3 packets.

Syntax

passive-interface { **default** | *interface-type interface-number* }

no passive-interface { **default** | *interface-type interface-number* }

Parameter Description

Default: Configures all interfaces as passive interfaces.

interface-type interface-number: Interface type and interface number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To prevent other routers in the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address. The loopback interface and the interface that is not connected to any OSPF neighbor can be set to passive interfaces.

When an interface is configured as a passive interface, it no longer sends or receives hello packets.

This command takes effect only on an OSPFv3 interface, and not on a virtual link.

Examples

The following example configures all interfaces of the local router as passive interfaces and enables OSPFv3 on the interfaces of VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface vlan 1
```

Notifications

If the specified interface is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf interface**

1.41 redistribute

Function

Run the **redistribute** command to enable route redistribution and inject routing information of other routing protocols to an OSPFv3 routing process.

Run the **no** form of this command to disable this function or modify the redistribution parameters.

The route redistribution function is not enabled by default.

Syntax

redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] * | **ospf** *process-id* [**match** { **externa**l [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** *metric-value* | **metric-type** { **1** | **2** } | **route-map** *route-map-name* | **tag** *tag-value*] *

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] * | **ospf** *process-id* [**match** { **externa**l [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** | **metric**-**type** | **route**-**map** | **tag**] *

Parameter Description

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

isis [*area-tag*]: Indicates redistribution from IS-IS. Here, *area-tag* specifies an IS-IS instance.

level-1 | **level-2** | **level-1-2**: Redistributes IS-IS routes at the specified level.

ospf *process-id*: Indicates redistribution from OSPF. Here, *process-id* specifies an OSPF process. The value range is from 1 to 65535.

match: Redistributes specific OSPFv3 routes that meet the filtering conditions.

external [**1** | **2**]: Redistributes E1, E2, or all external routes.

internal: Redistributes internal routes and inter-area routes.

nssa-external [**1** | **2**]: Redistributes N1, N2, or all external routes of all NSSAs.

rip: Indicates redistribution from RIP.

static: Indicates redistribution from static routes.

metric *metric-value*: Configures a metric value of OSPFv3 external LSAs, which is specified based on *metric-value*. The value range is from 0 to 16777214.

metric-type { **1** | **2** }: Configures the metric type of external routes, which can be E-1 or E-2.

route-map *route-map-name*: Configures the redistribution route filtering rules. Here, the value of *route-map-name* cannot exceed 32 characters.

tag *tag-value*: Specifies the tag value of the route that is redistributed to an OSPFv3 routing domain. The value range is from 0 to 4294967295.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the device supports multiple routing protocols, collaboration between protocols is required. To run multiple routing protocols concurrently, the device must be able to redistribute routing information of a protocol to another protocol.

During redistribution of IS-IS routes, **level-1**, **level-2**, or **level-1-2** parameters can be configured to indicate that IS routes of the specified levels are redistributed. By default, level-2 IS-IS routes are redistributed.

During redistribution of OSPFv3 routes, *match* can be configured to indicate that OSPFv3 routes of the specified sub-type are redistributed. By default, all types of OSPFv3 routes are redistributed.

For the **level** parameter configured for redistribution of IS-IS routes and the **match** parameter configured during redistribution of OSPFv3 routes, the routes are matched against the route map only when the sub-types of the routes are correct.

The **match** parameter in the route map rule used for route redistribution is matched based on the original information of the routes. The priority of the **tag**, **metric**, and **metric-type** parameters configured for route redistribution is lower than that of the **set** rule in the route map.

The **set metric** value of the associated route map should fall into the range of 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

The configuration rules for the **no** form of the **redistribute** command are as follows:

- If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
- If no parameter is specified in the **no** form of this command, the entire command will be deleted.

For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

Examples

The following example redistributes a direct route and associates the route with the route map **test**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# redistribute connect metric 10 route-map test
```

The following example configures the route map **test** and changes the metric value of the matched routes from **20** to **30** and the metric value of other redistributed routes from **20** to **10**.

```
Hostname(config)# route-map test permit 10
Hostname(config-route-map)# match metric 20
Hostname(config-route-map)# set metric 30
```

Notifications

If routes of this instance are redistributed, the following notification will be displayed:

```
% Redistribution of "ospf 1" via "ospf 1" not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf database**

1.42 router-id

Function

Run the **router-id** command to configure the ID of a router.

Run the **no** form of this command to remove this configuration.

A router ID is selected from IP addresses of interfaces by default. By default, the OSPFv3 routing process elects the largest IPv4 address among all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPFv3 process elects the largest one among the IP addresses of all its physical interfaces as the router ID.

Syntax

router-id *router-id*

no router-id

Parameter Description

router-id: ID of a router, which is expressed in the IPv4 address.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Every OSPFv3 router must be identified by using a router ID. You can configure an IPv4 address as the ID of the router, but ensure that the router ID is unique in an AS. If a router runs multiple OSPFv3 processes, ensure that the router ID of each process is unique.

After the router ID changes, OSPF performs a lot of internal processing. Therefore, you are not advised to change the router ID unless necessary. When an attempt is made to modify the router ID, a prompt is displayed, requesting you to confirm the modification. After an OSPFv3 process is enabled, you are advised to specify the router ID before configuring other parameters of the process.

Examples

The following example sets the router ID to 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# router-id 1.1.1.1
```

Notifications

When you set the router ID to 0.0.0.0, which stops the OSPFv3 process, the following notification will be displayed:

```
% OSPFv3: router-id set to 0.0.0.0, process will not run.
```

When the configured router ID is duplicate with that of another process, the following notification will be displayed:

```
% OSPFv3: router-id %r is in use by process %s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.43 show ipv6 ospf

Function

Run the **show ipv6 ospf** command to display information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of an OSPFv3 process.

```
Hostname> enable
Hostname# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
```

```
Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjency Changes : Enabled
BFD enabled
Number of areas in this router is 2
Area BACKBONE(0)
Number of interfaces in this area is 1(1)
SPF algorithm executed 4 times
Number of LSA 3. Checksum Sum 0x1DDF1
Number of Unknown LSA 0
Area 0.0.0.1 (NSSA)
Number of interfaces in this area is 1(1)
SPF algorithm executed 5 times
Number of LSA 7. Checksum Sum 0x445FE
Number of Unknown LSA 0
```

Table 1-1 Output Fields of the show ipv6 ospf Command

Field	Description
Routing Process "OSPFv3 (x)" with ID 1.1.1.1	OSPFv3 process ID and OSPFv3 router ID
Process uptime	Validation time of this OSPFv3 process (the process is invalid when the router ID is 0.0.0.0)
Enable two-way-maintain	Whether to enable two-way maintenance of OSPFv3
SPF schedule delay	Required delay time before calling the SPF computation when a topology change is received
SPF Hold time	Minimum holding time between two SPF computations
Initial LSA throttle delay	Minimum delay time of generating LSAs
Minimum hold time for LSA throttle	Minimum interval between two SPF computations
Maximum wait time for LSA throttle	Maximum interval between two SPF computations
Lsa Transmit Pacing timer	LSA group update frequency
Minimum LSA arrival	Minimum receiving delay time of LSAs

Field	Description
Pacing lsa-group	Group pace interval
Incomming current DD exchange neighbors	Number of neighbors in interaction. Incoming means that a neighbor enters the Exstart state for the first time.
Outgoing current DD exchange neighbors	Number of neighbors in interaction. Outgoing means that a neighbor returns from a higher state to the Exstart state for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Sum of checksums of external LSAs stored in the database
Number of AS-Scoped Unknown LSA	Number of unknown LSAs in the flooding scope
Number of LSA originated	Number of generated LSAs
Number of LSA received	Number of received LSAs
Log Neighbor Adjency Changes	Whether the neighbor state change recording is enabled
BFD enabled	Whether to associate OSPFv3 with BFD
Number of areas in this router	Number of areas on this router
Number of interfaces in this area	Number of interfaces in this area
SPF algorithm executed	SPF computation times
Number of LSA	Total number of LSAs in this area
Checksum Sum	Sum of the checksums of LSAs in this area
Number of Unknown LSA	Number of LSAs of unknown types received in this area
NSSA Translator State	Whether an NSSA LSA is translated to an external LSA. This field is valid only for the OSPFv3 process that is an ABR in the NSSA.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show ipv6 ospf database

Function

Run the **show ipv6 ospf database** command to display the database information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **database** [**database-summary** | *lsa-type* [**adv-router** *router-id*]]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

lsa-type: LSA type, including

NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs,

Intra-Area-Prefix-LSAs, Network-LSAs, and Router-LSAs.

If this parameter is not specified, all LSA information is displayed.

adv-route*r router-id*: Displays LSA information generated by a specified OSPFv3 neighbor.

database-summary: Displays the statistical information of each type of LSAs in the OSPFv3 LSDB.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the database information of an OSPFv3 process.

```
Hostname> enable
Hostname# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface GigabitEthernet 0/1)
Link State ID   ADV Router    Age   Seq#       CkSum    Prefix
0.0.0.2        1.1.1.1      197   0x80000001  0x7cd8   0
0.0.0.5        2.2.2.2      206   0x80000001  0x8c86   0
Link-LSA (Interface Loopback 1)
Link State ID   ADV Router    Age   Seq#       CkSum    Prefix
0.0.64.1       1.1.1.1      82    0x80000001  0xb760   0
Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#       CkSum    Link
0.0.0.0        1.1.1.1      17    0x80000006  0x62a1   1
0.0.0.0        2.2.2.2      156   0x80000003  0x8653   1
Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#       CkSum
```

```
0.0.0.5       2.2.2.2      157   0x80000001  0xf8f6
Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#       CkSum    Link
0.0.0.0       1.1.1.1      17    0x80000002  0x0529   0
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#       CkSum
0.0.0.1       1.1.1.1      77    0x80000002  0x83b4
AS-external-LSA
Link State ID   ADV Router    Age   Seq#       CkSum
0.0.0.1       1.1.1.1      1     0x80000001  0x6035 E2
```

Table 1-2 Output Fields of the show ipv6 ospf database Command

Field	Description
Link-LSA (Interface GigabitEthernet 0/1) Type-1 LSA—Router-LSA Type-2 LSA—Network-LSA Type-3 LSA—Inter-Area-Prefix-LSA Type-4 LSA—Inter-Area-Router-LSA Type-5 LSA—AS-External-LSA Type-7 LSA—NSSA-external-LSA Type-8 LSA—Link-LSA Type-9 LSA—Intra-Area-Prefix-LSA	Types of OSPFv3 Link-LSA
Link State ID	Link state ID of LSA
ADV Router	Advertising router of LSA
Age	LSA aging time
Seq#	LSA serial number
CkSum	LSA checksum
Prefix	Number of IPv6 address prefixes in Type-8 LSA
Link	Number of links in Type-1 LSA

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show ipv6 ospf interface

Function

Run the **show ipv6 ospf interface** command to display the information of an OSPFv3 interface.

Syntax

show ipv6 ospf [*process-id*] **interface** [**brief** | *interface-type interface-number*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

brief: Displays the brief information of an interface.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of an OSPFv3 interface.

```
Hostname> enable
Hostname# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1,
BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Table 1-3 Output Fields of the show ipv6 ospf interface Command

Field	**Description**
GigabitEthernet 0/1 is up, line protocol is up	Link and protocol state
Interface ID	Interface index
IPv6 Prefixes	IPv6 prefix information of an interface
OSPFv3 Process (1)	OSPFv3 process where an interface resides
Area	Area to which an interface belongs
Instance ID	Instance to which an interface belongs
Router ID	ID of an OSPFv3 router
Network Type	OSPFv3 network type
Cost	Cost of an OSPFv3 interface
Transmit Delay	Transmission delay of an OSPFv3 interface
State	DR/BDR state
Priority	Priority of an OSPFv3 interface
BFD enabled	Whether to associate OSPFv3 with BFD
Designated Router (ID)	ID for the DR of this interface
DR's Interface address	Interface address for the DR of this interface
Backup Designated Router (ID)	ID for the BDR of this interface
BDR's Interface address	Interface address for the BDR of this interface
Time intervals configured	Hello, Dead, Wait, and Retransmit time corresponding to this interface
Hello due in	Hello packet sending duration last time
Neighbor Count	Total number of neighbors
Adjacent neighbor count	Number of neighbors in full neighbor relationship
Hello received sent	Statistics of the received and sent hello packets
DD received send	Statistics of the received and sent DD packets
LS-Req received send	Statistics of the received and sent LS request packets
LS-Upd received send	Statistics of the received and sent LS update packets
LS-Ack received send	Statistics of the received and sent LS response packets

Field	Description
Discard	Statistics of the discarded OSPFv3 packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 show ipv6 ospf neighbor

Function

Run the **show ipv6 ospf neighbor** command to display neighbor information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **neighbor** [**detail** | *interface-type interface-number* [**detail**] | *neighbor-id* | **statistics**]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

detail: Displays the neighbor details.

interface-type interface-number: Interface type and interface number.

neighbor-id: Route ID of a specified neighbor.

statistics: Displays the statistics of neighbors.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the brief information of an OSPFv3 neighbor.

```
Hostname> enable
Hostname# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State    Dead Time   Interface       Instance ID
```

```
2.2.2.2     1    Full/DR   00:00:33    GigabitEthernet 0/1  0
Hostname# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface GigabitEthernet 0/1
Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

Table 1-4 Output Fields of the show ipv6 ospf neighbor Command

Field	Description
OSPFv3 Process (1), 1 Neighbors, 1 is Full:	Process ID, number of neighbors, and number of neighbors in full neighbor relationship
Neighbor ID	Router ID of a neighbor
Pri	Priority of a neighbor

Field	Description
State	Neighbor states, including Down—Initial status of a neighbor in a session Attempt—When the interface of a device in the NBMA qualified for DR election becomes valid, the neighbor state is reset to Attempt. This state is applicable to neighbors in the NBMA. Init—The neighbor receives a hello packet that does not contain the neighbor ID. 2-Way—The hello packet received from the neighbor contains the local router ID, indicating that 2-way communication has been established. Exstart—An active/standby relationship is established between a router and its neighbors and the sequence number of DD packets is determined, which is ready for DD packet exchange. Exchange—A router sends DD packets that describe local LSDB information to its neighbors. Loading—A router sends LSR packets to a neighbor to request the latest LSA. Full—A router establishes full adjacency relationship with neighbors. OSPF routers play the following roles in broadcast and NBMA networks: DR—A DR exists in only broadcast and NBMA networks. BDR—A BDR exists in only broadcast and NBMA networks. DRother—Indicates all other devices except the DR and BDR in broadcast and NBMA networks. In P2P and P2MP networks, the preceding roles do not exist, and this field is displayed as a hyphen (-).
Dead Time	Time before the neighbor enters the dead state
Instance ID	ID of a neighbor instance
Interface	Interface connected to neighbors
Interface address	Interface address of the neighbor router
In the area	Area that learns this neighbor
via interface	Interface that learns this neighbor
Neighbor priority	Priority value of the neighbor
State changes times	Change times of the neighbor state
DR	Interface address (namely, the DR field in the hello packet) of the DR elected by the neighbor router
BDR	Interface address (namely, the BDR field in the hello packet) of the BDR elected by the neighbor router

Field	Description
Options	Options for the hello packet
Dead Time due in	Time when the dead state of this neighbor is declared
Database Summary List	DD packet statistics of the neighbor
Link State Request List	LSR packet statistics of the neighbor
Link State Retransmission List	Retransmitted packet statistics of the neighbor
BFD session state up	BFD association state

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 show ipv6 ospf restart

Function

Run the **show ipv6 ospf restart** command to display the information related to OSPFv3 GR.

Syntax

show ipv6 ospf [*process-id*] **restart**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the current status of the restarter.

```
Hostname> enable
```

```
Hostname# show ipv6 ospf restart
Routing Process is ospf 1
Graceful-restart enabled
Restart grace period 120 secs
Current Restart status is plannedRestart
Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

Table 1-5 Output Fields of the show ipv6 ospf restart Command

Field	Description
Routing Process is ospf	ID of a process that starts GR
Graceful-restart enabled	Whether to enable the GR function
Restart grace period	GR period
Current Restart status	Current GR status
Current Restart remaining time	Remaining GR time
Graceful-restart helper support enabled	Whether to support restart helper

The following example displays the current status of the restart helper.

```
Hostname> enable
Hostname# show ipv6 ospf restart
Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

Table 1-6 Output Fields of the show ipv6 ospf restart Command

Field	Description
Neighbor	Router ID of the neighbor of the helper
interface addr	IP address of the interface corresponding to the helper
In the area	Area in which the helper resides
interface GigabitEthernet	Interface corresponding to the helper
Graceful-restart helper enabled	Whether to enable the helper function
Current helper status	Current helper status
Current helper remaining time	Remaining time of a router in the helper state

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 show ipv6 ospf route

Function

Run the **show ipv6 ospf route** command to display the routing information of OSPFv3.

Syntax

show ipv6 ospf [*process-id*] **route** [**count**]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

count: Displays the number of OSPFv3 routes.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the routing information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, B – Backup O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2Destination        Metric
Next-hop
E2 2001:DB8:1::/64   1/20    via fe80::c800:eff:fe84:1c, GigabitEthernet 0/1
B                        via fe80::c800:eff:fe84:1d, GigabitEthernet 0/2
O  2001:DB8:2::/64   11      via fe80::c800:eff:fe84:1c, GigabitEthernet 0/1, Area
0.0.0.0
```

Table 1-7 Output Fields of the show ipv6 ospf route Command

Field	Description
OSPFv3 Process (1)	OSPFv3 process ID
Destination	Type and destination network of OSPFv3 routes OSPFv3 supports the following four types of routes: **C**: Direct route **D**: Black-hole route **O**: Internal route of OSPFv3 **IA**: Inter-area route of OSPFv3 **N1**: NSSA external type 1 route of OSPFv3 **N2**: NSSA external type 2 route of OSPFv3 **E1**: External type 1 route of OSPFv3 **E2**: External type 2 route of OSPFv3
Metric	Cost of a route
Next-hop	Next hop of a route

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 show ipv6 ospf summary-prefix

Function

Run the **show ipv6 ospf summary-prefix** command to display external route summarization information of OSPFv3.

Syntax

show ipv6 ospf [*process-id*] **summary-prefix**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the external route summarization information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:1::/64, Metric 20, Type 2, Tag 0, Match count 5, advertise
```

Table 1-8 Output Fields of the show ipv6 ospf summary-prefix Command

Field	Description
Summary-prefix	Prefix of a summarized route
Metric	Metric of a summarized route
Type	Type of a summarized route
Match count	Number of summarized routes
Advertise	Advertisement after summarization
Tag	Tag of a summarized route

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.50 show ipv6 ospf topology

Function

Run the **show ipv6 ospf topology** command to display the topological information of an OSPFv3 area.

Syntax

show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the topological information of an OSPFv3 area.

```
Hostname> enable
Hostname# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID       Bits  Metric    Interface           Next-Hop(router/address)
1.1.1.1           B
2.2.2.2          EB  1        GigabitEthernet 0/6
2.2.2.2/fe80::21a:a9ff:fe41:5b06
OSPFv3 paths to Area (0.0.0.1) routers
Router ID       Bits  Metric    Interface           Next-Hop(router/address)
1.1.1.1          V B
2.2.2.2          VEB  1        GigabitEthernet 0/6
2.2.2.2/fe80::21a:a9ff:fe41:5b06
```

Table 1-9 Output Fields of the show ipv6 ospf topology Command

Field	Description
OSPFv3 paths to Area	Topological information corresponding to an area
Router ID	Router ID of a node
Bits	Options for a node
Metric	Metric from this node to the root node
Interface	Outbound interface to this node
Next-Hop(router/address)	Next hop to this node

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 show ipv6 ospf virtual-links

Function

Run the **show ipv6 ospf virtual-links** command to display virtual link information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **virtual-links**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays virtual link information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/1, instance ID 0
  Local address 2001::2/128
  Remote address 2001::1/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
Adajcency state Full
```

Table 1-10 Output Fields of the show ipv6 ospf virtual-links Command

Field	Description
Virtual Link VLINK1 to router	Neighbor and neighbor state of a virtual link
Transit area	Transmission area of a virtual link
via interface	Interface associated with a virtual link
Local address	Address of the local interface

Field	Description
Remote address	Address of the peer interface
Transmit Delay	Transmission delay of a virtual link
State	Network type of a virtual link
Timer intervals configured	Timer of a virtual link, including Hello, Dead, and Retransmit
Hello due in	Hello packet sending interval
Adjacency state	Neighbor state of a virtual link

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 summary-prefix

Function

Run the **summary-prefix** command to configure a summarized route for the external routes of an OSPFv3 routing domain.

Run the **no** form of this command to restore the default configuration.

Route summarization is disabled by default.

Syntax

summary-prefix *ipv6-prefix*/*prefix-length* [[**cost** *cost* | **tag** *tag-value*] * | **not-advertise**]

no summary-prefix *ipv6-prefix*/*prefix-length* [[**cost** | **tag**] ***** | **not-advertise**]

Parameter Description

ipv6-prefix/prefix-length: Range of IP addresses to be summarized.

cost *cost*: Configures a cost value of the summarized routes. The value range is from 0 to 16777214. The default metric value is the minimum cost value of the summarized routes.

tag *tag-value*: Specifies the tag value of the route that is redistributed to an OSPFv3 routing domain. The value range is from 0 to 4294967295.

not-advertise: Does not advertise this summarized route to neighbors. If this parameter is not specified, this summarized route is advertised.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When routes are redistributed from other routing processes and injected to the OSPFv3 routing process, each route is advertised to the OSPFv3 routers using an external LSA. If the injected routes are a continuous address space, the ASBR can advertise only one summarized route to reduce the size of the routing table.

While **area range** summarizes the routes between OSPFv3 areas, **summary-prefix** summarizes external routes of the OSPFv3 routing domain.

When configured on the NSSA ABR translator, **summary-prefix** summarizes redistributed routes and routes obtained based on the LSAs that are translated from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-prefix** summarizes only redistributed routes.

Examples

The following example summarizes external routes of the OSPFv3 routing domain as 2001:DB8::/64 and advertises the routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# summary-prefix 2001:db8::/64
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf summary-prefix**

1.53 timers lsa arrival

Function

Run the **timers lsa arrival** command to configure the delay for receiving same LSAs.

Run the **no** form of this command to restore the default configuration.

By default, the delay for receiving a duplicate LSA is **1000** ms.

Syntax

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

arrival-time: Delay for receiving same LSAs, in milliseconds. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

No processing is performed if the same LSAs are received within the specified time to avoid resource consumption.

Examples

The following example sets the delay for receiving the same LSAs to **2** seconds at least.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers lsa arrival 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.54 timers pacing lsa-group

Function

Run the **timers pacing lsa-group** command to configure a group update time of LSAs.

Run the **no** form of this command to restore the default configuration.

The default group refresh time of LSAs is **30** seconds.

Syntax

timers pacing lsa-group *update-time*

no timers pacing lsa-group

Parameter Description

update-time: Group update time of LSAs, in seconds. The value range is from 10 to 1800.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, the LSA age must be updated to prevent LSAs from being cleared because their age reaches the maximum time to live. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources.

To use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole.

If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs to be processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Examples

The following example sets the LSA group refresh time to 120 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers pacing lsa-group 120
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.55 timers pacing lsa-transmit

Function

Run the **timers pacing lsa-transmit** command to configure the LSA group sending interval.

Run the **no** form of this command to restore the default configuration.

The default LSA group sending interval is **40** ms, and the number of LS-UPD packets in each group is **1**.

Syntax

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

transmit-time: LSA group sending interval, in milliseconds. The value range is from 10 to 1000.

transmit-count: Number of LS-UPD packets in each group. The value range is from 1 to 200.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transimit-time* and *transimit-count* can limit the number of LS-UPD packets flooded in the network.

If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transimit-time* and increasing the value of *transimit-count* can accelerate the environment convergence.

Examples

The following example sets the LSA group sending interval to **50** ms and the number of LS-UPD packets in each group to **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers pacing lsa-transmit 50 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.56 timers spf

Function

Run the **timers spf** command to configure the delay time for SPF computation after an OSPFv3 process receives the topological change information and the interval between two SPF computations.

Run the **no** form of this command to restore the default configuration.

By default, the **timers spf** command does not take effect, and the delay for SPF computation is subject to the default configuration of the **timers throttle spf** command. Refer to the description of the **timers throttle spf** command.

Syntax

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

spf-delay: Delay for SPF computation, in seconds. After receiving the topological change information, the OSPF routing process must wait for the specified time before performing SPF computation. The value range is from 0 to 2147483647.

spf-holdtime: Interval between two SPF computations, in seconds. If the delay time expires but the interval between two SPF computations does not expire, SPF computation still cannot be performed. The value range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Changes to LSDB will trigger SPF computation. Frequent network jitter will consume a lot of CPU resources. Setting a proper delay for SPF computation can avoid occupying excessive device memory and bandwidth resources.

Smaller values of *spf-delay* and *spf-holdtime* mean that the OSPF can adapt to topological changes more quickly. In other words, a shorter network convergence time means that more CPU time of the router will be occupied.

The configurations of **timers spf** and **timers throttle spf** are mutually overwritten.

Examples

The following example sets the delay time for SPF computation to **3** seconds after an OSPFv3 process receives the topological change information, and sets the interval between two SPF computations to **9** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 20
Hostname(config-router)# timers spf 3 9
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.57 timers throttle lsa all

Function

Run the **timers throttle lsa all** command to configure an exponential backoff algorithm of LSA packet generation.

Run the **no** form of this command to restore the default configuration.

The default minimum delay of LSA generation is **0** ms, the minimum interval between the first update and the second update of LSA is **5000** ms, and the maximum interval between consecutive LSA updates is **5000** ms.

Syntax

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

delay-time: Minimum delay for LSA generation, in milliseconds. The first LSA in the database is always generated instantly. The value range is from 0 to 600000.

hold-time: Minimum interval between the first LSA update and the second LSA update, in milliseconds. The value range is from 0 to 600000.

max-wait-time: Maximum interval between two LSA updates when the LSA is updated continuously, in milliseconds. This interval is also used to determine whether the LSA is updated continuously. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a high convergence requirement is raised when a link changes, you can set *delay-time* to a smaller value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage. When this command is used for configuration, the value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.

Examples

The following example sets the minimum delay of LSA generation to **10** ms, the minimum interval between the first update and the second update to **1** second, and the maximum interval between two LSA updates to **5** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers throttle lsa all 10 1000 5000
```

Notifications

If the configured value of *max-wait-time* is smaller than that of *hold-time*, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5)
```

If the configured value of *hold-time* is smaller than that of *delay-time*, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

- The configured value of *hold-time* is smaller than that of *delay-time* or the configured value of *max-wait-time* is smaller than that of *hold-time*.

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.58 timers throttle route

Function

Run the **timers throttle route** command to configure the delay time for route computation when an OSPFv3 process receives changed inter-area and external LSAs.

Run the **no** form of this command to restore the default configuration.

The default delay for inter-area route computation and external route computation is **0** ms.

Syntax

timers throttle route { **ase** *ase-delay* | **inter-area** *ia-delay* }

no timers throttle route { **ase** | **inter-area** }

Parameter Description

ase: Indicates external route computation.

ase-delay: Delay for external route computation, in milliseconds. When the OSPF process receives external LSA change information, the route computation triggered should be performed at least after the ase-delay for external route computation elapses. The value range is from 0 to 600000.

inter-area: Indicates inter-area route computation.

ia-delay: Delay for inter-area route computation, in milliseconds. When the OSPF process receives inter-area LSA change information, the route computation triggered should be performed at least after the ia-delay for inter-area route computation elapses. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a strict requirement is raised for the network convergence time, use the default value.

If a lot of inter-area or external routes exist in the network and the network is not stable, adjust the delays and optimize route computation to reduce the load on the device.

Examples

The following example sets the delay for inter-area route computation to **1** second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers throttle route inter-area 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.59 timers throttle spf

Function

Run the **timers throttle spf** command to configure the delay time for SPF computation when an OSPFv3 process receives topological change information, and the minimum and maximum intervals for two SPF computations.

Run the **no** form of this command to restore the default configuration.

The default delay for SPF computation is **1000** ms, the minimum interval for two SPF computations is **5000** ms, and the maximum interval between two SPF computations is **10000** ms.

Syntax

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

spf-delay: Delay for SPF computation, in milliseconds. When the OSPF process receives topological change information, the SPF computation triggered should be performed at least after the spf-delay for SPF computation elapses. The value range is from 1 to 600000.

spf-holdtime: Minimum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

spf-max-waittime: Maximum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Here, *spf-delay* indicates the minimum time between the occurrence of a topology change and the start of SPF computation. *spf-holdtime* indicates the minimum interval between the first and second SPF computations. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches *spf-max-waittime*, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval for SPF computation is computed starting from *spf-holdtime*.

You can set *spf-delay* and *spf-holdtime* to values smaller than the default values to accelerate topology convergence. The value of *spf-max-waittime* can be set to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology.

Compared with the **timers spf** command, this command supports more flexible settings to accelerate SPF computation convergence and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration.

Notes:

- The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, the value of *spf-holdtime* will be automatically set to the value of *spf-delay*.
- The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
- The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
- When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Examples

The following example sets the delay for SPF computation, hold time, and maximum interval for two SPF computations to 5 ms, 1000 ms, and 90000 ms, respectively. If the topology continuously changes, the delay for SPF computation is set to 5 ms, 1s, 3s, 7s, 15s, 31s, 63s, 89s, 179s, and (179+90)s..., respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 20
Hostname(config-router)# timers spf 5 1000 90000
```

Notifications

If the configured value of *max-wait-time* is smaller than that of *hold-time*, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

If the configured value of *hold-time* is smaller than that of *delay-time*, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.60 two-way-maintain

Function

Run the **two-way-maintain** command to enable the two-way maintenance function of OSPFv3.

Run the **no** form of this command to disable this function.

The two-way maintenance function of OSPFv3 is enabled by default.

Syntax

two-way-maintain

no two-way-maintain

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the neighbor dead interval, the adjacency will be destroyed due to timeout. If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist in the network. This prevents termination of the adjacency caused by delayed or discarded hello packets.

Examples

The following example enables the two-way maintenance function of an OSPF process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# no two-way-maintain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1 IS-IS Commands

Command	Function
address-family ipv6	Enter the IS-IS IPv6 address family configuration mode.
adjacency-check	Enable the neighbor supported protocol detection function in Hello packets.
area-password	Configure plaintext authentication password of Level-1 areas.
authentication key-chain	Configure a key chain for IS-IS authentication.
authentication mode	Enable an IS-IS authentication mode.
authentication send-only	Apply a specified IS-IS authentication mode to only sent packets. Received packets are not authenticated.
bandwidth-reference	Configure the reference bandwidth value of IS-IS.
bfd all-interfaces	Enable BFD for IS-IS interfaces.
clear clns neighbors	Clear all neighbor relationship tables of IS-IS.
clear isis *	Clear all data structures of IS-IS.
clear isis counter	Clear statistical information of IS-IS.
default-information originate	Generate a default route and advertise the route in LSPs.
distance	Configure the administrative distance of an IS-IS route.
domain-password	Configure plaintext authentication password of Level-2 areas.
enable mib-binding	Bind an IS-IS instance for SNMP operation.
enable traps	Enable the trap message sending function of IS-IS.
exit-address-family	Exit the IS-IS IPv6 address family configuration mode and go back to the IS-IS routing process configuration mode.
graceful-restart	Enable the GR capability of IS-IS.
graceful-restart grace-period	Configure the maximum GR interval of a device.

graceful-restart helper disable	Disable the IS-IS GR Helper capability.
hello padding	Enable padding specified IS-IS Hello packets.
hostname dynamic	Replace the system ID of a device with the host name of the destination device.
ignore-lsp-errors	Ignore LSP checksum errors.
interfaces-protocol-compatible	Pad the TLV field of the IS-IS protocol based on protocols supported by an interface.
ip router isis	Enable the IPv4 IS-IS routing function on an interface.
ipv6 router isis	Enable the IPv6 IS-IS routing function on an interface.
isis authentication key-chain	Configure a key chain for IS-IS interface authentication.
isis authentication mode	Enable an authentication mode of an IS-IS interface.
isis authentication send-only	Apply a specified IS-IS interface authentication mode to only sent packets. Received packets are not authenticated.
isis bfd	Enable IS-IS correlation with BFD on an interface.
isis circuit-type	Configure an IS-IS level on an interface.
isis csnp-interval	Specify the CSNP broadcast interval on an IS-IS interface.
isis hello padding	Enable padding IS-IS hello packets sent on an IS-IS interface.
isis hello-interval	Configure the hello packet sending interval on an interface.
isis hello-multiplier	Configure the multiplier of the hello holdtime on an interface.
isis lsp-flood	Configure the maximum number of LSP packets sent by the IS-IS interface at a time.
isis lsp-interval	Configure the LSP sending interval on an interface.
isis mesh-group	Add an IS-IS interface to a specified mesh group.
isis metric	Configure the metric for an IS-IS interface.

isis network point-to-point	Change the type of an interface from broadcast to P2P.
isis passive	Configure an interface as a passive interface.
isis password	Configure the password for plaintext authentication of hello packets on an interface.
isis priority	Configure the priority for DIS election in a LAN.
isis psnp-interval	Configure the minimum PSNP sending interval.
isis retransmit-interval	Configure the LSP retransmission interval on an IS-IS interface.
isis subvlan	Enable the IS-IS function in a super VLAN.
isis suppress on-neighbor-up	Suppress routing calculation after an IS-IS neighbor is up.
isis three-way-handshake disable	Disable three-way handshake of a P2P network.
isis wide-metric	Configure the wide metric value for an interface.
is-name	Replace the system ID of an instance with the configured name.
is-type	Specify the level at which IS-IS runs.
log-adjacency-changes	Record neighbor state changes of IS-IS without enabling the debug command.
lsp-fragments-extend	Enable fragment extension.
lsp-gen-interval	Configure an exponential backoff algorithm of LSP generation.
lsp-length originate	Configure the maximum length of sent LSPs.
lsp-length receive	Configure the maximum length of received LSPs.
lsp-refresh-interval	Configure the LSP refresh interval.
max-area-addresses	Configure the maximum number of area addresses.
maximum-paths	Configure the maximum number of IS-IS equal-cost paths to be added to a routing table.
max-lsp-lifetime	Configure the maximum LSP lifetime.
max-metric on-neighbor-up	Configure the maximum metric for the directly-connected routes after the first neighbor is up.

metric-style	Configure a metric type.
min-lsp-arrival	Configure the delay for receiving duplicate LSPs.
multi-topology	Configure IS-IS to support IPv6 unicast topologies. After that, IPv4 and IPv6 unicast routes in IS-IS will be calculated based on different topologies.
net	Configure a NET address in IS-IS.
nsr	Enable the NSR function for current IS-IS instance.
passive-interface	Configure a passive interface.
redistribute	Redistribute other routes to IS-IS.
redistribute isis level-1 into level-2	Redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.
redistribute isis level-2 into level-1	Redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.
router isis	Create an IS-IS instance.
set-overload-bit	Prevent neighbors from using the local IS-IS node as a forwarding device to forward data.
show clns is-neighbors	Display all IS-IS neighbors and provide device adjacency relationship information.
show clns neighbors	Display all IS-IS neighbors and provide device information and adjacency relationship information about terminals.
show isis counter	Display statistical information of IS-IS.
show isis database	Display the information of an LSP database.
show isis graceful-restart	Display the state information about IS-IS GR.
show isis hostname	Display the mapping of a host name to a system ID.
show isis interface	Display details of an IS-IS interface.
show isis ipv6 topology	Display the IPv6 unicast topology information of an IS-IS device.
show isis mesh-groups	Display the mesh group configuration of interfaces.
show isis neighbors	Display neighbor information of IS-IS.
show isis nsr	Display NSR information of IS-IS.

show isis protocol	Display protocol information of IS-IS.
show isis topology	Display the topology information of connected IS-IS devices.
show isis virtual-neighbors	Display virtual system neighbor information of IS-IS.
spf-interval	Configure the exponential backoff algorithm of SPF calculation.
summary-address	Configure IPv4 summarized routes.
summary-prefix	Configure IPv6 summarized routes.
two-way-maintain	Enable the two-way maintenance function of IS-IS.
virtual-system	Configure an additional system ID for fragment extension.
vrf	Bind an IS-IS instance to a VRF table.

1.1 address-family ipv6

Function

Run the **address-family ipv6** command to enter the IS-IS IPv6 address family configuration mode.

Run the **no** form of this command to remove this configuration.

A device does not enter the IPv6 address family configuration mode by default.

Syntax

address-family ipv6 [**unicast**]

no address-family ipv6 [**unicast**]

Parameter Description

unicast: Specifies to use the IPv6 unicast address prefix of the IPv6 address family. This parameter is optional and does not make any difference no matter whether it is configured.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Run this command to enter the IS-IS IPv6 address family configuration mode. Special IS-IS IPv6 configuration can be made in this mode.

To exit the IS-IS IPv6 address family configuration mode, run the **exit-address-family** command.

Examples

The following example enters the IS-IS IPv6 address family configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6 unicast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **router isis**

1.2 adjacency-check

Function

Run the **adjacency-check** command to enable the neighbor supported protocol detection function in Hello packets.

Run the **no** form of this command to disable this function.

The neighbor supported protocol detection function for hello packets is enabled by default.

Syntax

adjacency-check

no adjacency-check

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the neighbor supported protocol detection function in hello packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# no adjacency-check
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# no adjacency-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 area-password

Function

Run the **area-password** command to configure plaintext authentication password of Level-1 areas.

Run the **no** form of this command to remove this configuration.

The authentication password configuration function is disabled by default.

Syntax

area-password [**0** | **7**] *password-string* [**send-only**]

no area-password [**send-only**]

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticated.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-1 areas and include authentication information in these packets before they are sent. All IS-IS devices in an area must be configured with the same *password-string*.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no area-password** command. If you run the **no area-password send-only** command, only the **send-only** setting is canceled. If you run the **area-password** *psw* **send-only** and **no area-password send-only** commands in sequence, the configuration is changed to **area-password** *psw*.

Examples

The following example sets the plaintext authentication password of Level-1 areas to **redgiant** and applies the password to only sent packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
```

```
Hostname(config-router)# area-password redgiant send-only
```

Notifications

If authentication is configured using the **authentication mode** command, the following notification will be displayed:

```
% Please configure password using authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 authentication key-chain

Function

Run the **authentication key-chain** command to configure a key chain for IS-IS authentication.

Run the **no** form of this command to remove this configuration.

The authentication key chain function is disabled by default.

Syntax

authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

name-of-chain: Name of a key chain. The maximum length is 255.

level-1: Indicates that the authentication key chain takes effect for Level-1.

level-2: Indicates that the authentication key chain takes effect for Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Authentication is not performed if no key chain is configured using the **key chain** command.

(1) If the **authentication mode** command is run with this command, the authentication type configured in the **authentication mode** command is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **authentication mode** command to specify the authentication mode.

(2) If only this command is run, the authentication type specified by the key-chain is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **key chain** command to specify the authentication mode.

For plaintext authentication, the key-string in the key chain cannot exceed 80 characters; otherwise, the key chain will be invalid.

Only one key chain can be used at a time. After you configure a new key chain, it will replace the original one.

If no Level is specified, the key chain takes effect for Level-1 and Level-2.

The key chain is applicable to LSPs, CSNPs, and PSNPs. IS-IS will send or receive passwords that belong to the key chain.

A key chain may contain multiple passwords. A password with a smaller SN is preferentially used for sending a packet. When the packet arrives at the peer device, the device will receive the packet if the packet-carried password is consistent with a password in the key chain.

If key chain authentication is configured and the authentication type specified in the key chain is SM3, the range of Algorithm-ID is 0 to 255. If the Algorithm-ID exceeds the range, IS-IS packets do not carry TLV information for authentication. In this case, local authentication and checking will fail.

Examples

The following example specifies the Level-1 key chain with the name kc for IS-IS authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication key-chain kc level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **authentication mode**

1.5 authentication mode

Function

Run the **authentication mode** command to enable an IS-IS authentication mode.

Run the **no** form of this command to disable this mode.

The authentication mode function is disabled by default.

Syntax

authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no authentication mode { **md5** | **text** } [**level-1** | **level-2**]

Parameter Description

md5: Specifies the MD5 authentication mode.

text: Specifies the plaintext authentication mode.

level-1: Specifies that the authentication mode takes effect for Level-1.

level-2: Specifies that the authentication mode takes effect for Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

If you use the **authentication mode** command after the **area-password** or **domain-password** command is executed to configure plaintext authentication, the previous command configuration will be overwritten.

The **area-password** or **domain-password** command does not take effect if the **authentication mode** command is executed. To run the **area-password** or **domain-password** command, delete the **authentication mode** command configuration first.

Examples

The following example specifies the IS-IS authentication mode as MD5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication mode md5 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 authentication send-only

Function

Run the **authentication send-only** command to apply a specified IS-IS authentication mode to only sent packets. Received packets are not authenticated.

Run the **no** form of this command to restore the default configuration.

Packets sent and received are authenticated by default.

Syntax

authentication send-only [**level-1** | **level-2**]

no authentication send-only [**level-1** | **level-2**]

Parameter Description

level-1: Applies authentication to only the sent packets on Level-1.

level-2: Applies authentication to only the sent packets on Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to enable IS-IS to set an authentication password in the Hello packets to be sent. Received packets are not authenticated. You can use this command before you deploy IS-IS authentication on all devices in the network or before you change the authentication password or authentication mode. Before using this command, you should run the **authentication send-only** command. The devices will not authenticate received packets to avoid network flapping during authentication deployment. After authentication is deployed in the entire network, run the **no isis authentication send-only** command to cancel the **send-only** setting.

This command is applicable to plaintext authentication and MD5 authentication. You can run the **authentication mode** command to specify the authentication mode.

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

Examples

The following example specifies that IS-IS authentication is performed only on sent packets. Received packets are not authenticated.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication send-only level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis database**

1.7 bandwidth-reference

Function

Run the **bandwidth-reference** command to configure the reference bandwidth value of IS-IS.

Run the **no** form of this command to remove this configuration.

The default reference bandwidth value for cost computation is **100** Mbps.

Syntax

bandwidth-reference *bandwidth*

no bandwidth-reference

Parameter Description

bandwidth: Reference bandwidth value for automatic cost computation of an IS-IS link, in Mbps. The value range is from 1 to 4294967.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If an IS-IS interface is configured with a metric value, the bandwidth value in this command does not involve in cost computation of a link.

Examples

The following example sets the reference bandwidth value of IS-IS to **200** Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# bandwidth-reference 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to enable BFD for IS-IS interfaces.

Run the **no** form of this command to disable this function.

The IS-IS correlation with BFD function is disabled on all interfaces by default.

Syntax

bfd all-interfaces [**anti-congestion**]

no bfd all-interfaces [**anti-congestion**]

Parameter Description

anti-congestion: Indicates the IS-IS BFD anti-congestion option.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

You can enable or disable BFD on an IS-IS interface by using any of the following two methods:

Method 1: Run the [**no**] **bfd all-interfaces** [**anti-congestion**] command in IS-IS routing process configuration mode to enable or disable BFD on all IS-IS interfaces.

Method 2: Run the **isis bfd** [**disable** | **anti-congestion**] command in interface configuration mode to enable or disable BFD on the specified interface.

Normally, BFD sends detection packets at millisecond intervals to detect the link state. When a link exception (such as a disconnected link) occurs, BFD can quickly detect it and instruct IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Then IS-IS recalculates and generates a new route to bypass the abnormal link, thus realizing fast convergence. With many new techniques such as Multi-Service Transport Platform (MSTP) emerging, links become easily congested in peak hours of data communication. In this case, BFD can quickly detect the abnormal link and instruct IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Link switch is performed to bypass the congested link. A Hello packet for IS-IS neighbor detection is sent every 10s and its expiration time is 30s. The Hello packet can still be received normally when BFD detects an exception, and therefore an IS-IS neighbor relationship is reestablished quickly, causing the route to be restored to the congested link. Then BFD detects the abnormal link and link switch is performed again. This process is repeated, which makes the route be switched between the congested link and other links, causing repetitive flapping.

The anti-congestion option is used to avoid route flapping in case of link congestion. After the option is configured, the IS-IS neighbor state is still kept alive when link congestion occurs, but the neighbor reachability information in LSPs is deleted. The route is switched to a normal link. When the congested link is restored, the neighbor reachability information in LSPs is recovered and the route is switched back, which avoids route flapping.

When you run the **bfd all-interfaces [anti-congestion]** command, you must run the **bfd up-dampening** command on the interface. The two commands must be used together. If you run only one command, the anti-congestion feature may not take effect or other network exceptions may occur.

Note

- You must configure a BFD session on the interface before you enable IS-IS correlation with BFD.
- When you run the **bfd up-dampening** command on an interface with IS-IS correlation with BFD, you must run the **bfd all-interfaces [anti-congestion]** command.
- When you run the **bfd all-interfaces** command with the **[anti-congestion]** option selected, run the **bfd up-dampening** command on the interface.

Examples

The following example configures all interfaces running IS-IS protocol to perform BFD for link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 123
Hostname(config-router)# bfd all-interface
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bfd up-dampening** (reliability/BFD)

1.9 clear clns neighbors

Function

Run the **clear clns neighbors** command to clear all neighbor relationship tables of IS-IS.

Syntax

clear clns neighbors

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to refresh the neighbor relationship tables of IS-IS immediately.

Examples

The following example clears all neighbor relationship tables of IS-IS.

```
Hostname> enable
Hostname# clear clns neighbors
```

Notifications

N/A

Platform Description

N/A

1.10 clear isis *

Function

Run the **clear isis *** command to clear all data structures of IS-IS.

Syntax

clear isis *

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to refresh LSPs immediately. After the **area-password** and **domain-password** commands are run, if old LSPs remain existent in the local device, you can use this command to clear these LSPs.

Examples

The following example clears all data structures of IS-IS.

```
Hostname> enable
Hostname# clear isis *
```

Notifications

N/A

Platform Description

N/A

1.11 clear isis counter

Function

Run the **clear isis counter** command to clear statistical information of IS-IS.

Syntax

clear isis [*tag*] **counter**

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to clear statistical information of IS-IS.

Examples

The following example clears statistical information of IS-IS.

```
Hostname> enable
Hostname# clear isis counter
```

Notifications

N/A

Platform Description

N/A

1.12 default-information originate

Function

Run the **default-information originate** command to generate a default route and advertise the route in LSPs.

Run the **no** form of this command to remove this configuration.

The default route function is disabled by default.

Syntax

default-information originate [**route-map** *route-map-name*]

no default-information originate

Parameter Description

route-map *route-map-name*: Associates a route map.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

Because Level-2 domains do not generate any default route, use this command to allow a default route to enter a Level-2 domain.

Examples

The following example generates a default route and advertises the route in LSPs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# default-information originate
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# default-information originate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis database**

1.13 distance

Function

Run the **distance** command to configure the administrative distance of an IS-IS route.

Run the **no** form of this command to restore the default configuration.

The default administrative distance of IS-IS is **115**.

Syntax

distance *distance-value*

no distance

Parameter Description

distance-value: Administrative distance of a route. The value range is from 1 to 255.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

If the administrative distance of a route is set to a smaller value, the routing information becomes more trustworthy and the priority of the route in the routing table is higher.

Examples

The following example sets the administrative distance of an IS-IS route to **100** Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# distance 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 domain-password

Function

Run the **domain-password** command to configure plaintext authentication password of Level-2 areas.

Run the **no** form of this command to remove this configuration.

The Level-2 domain authentication password function is disabled by default.

Syntax

domain-password [**0** | **7**] *password-string* [**send-only**]

no domain-password [**send-only**]

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-2 areas. Received Hello packets are not authenticated.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-2 areas and include authentication information in these packets before they are sent. All IS-IS devices in a Level-2 area must be configured with the same *password-string*.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no domain-password** command. If you run the **no domain-password send-only** command, only the **send-only** setting is canceled. If you run the **domain-password** *psw* **send-only** and **no domain-password send-only** commands in sequence, the configuration is changed to **domain-password** *psw*.

Examples

The following example sets the plaintext authentication password of Level-2 domain to **redgiant**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# domain-password redgiant
```

Notifications

If authentication has been configured for Level-2 area by the **authentication mode** command, the following notification will be displayed:

```
% Please configure password using authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 enable mib-binding

Function

Run the **enable mib-binding** command to bind an IS-IS instance for SNMP operation.

Run the **no** form of this command to remove this configuration.

By default, the SNMP operation is performed on the first displayed IS-IS instance.

Syntax

enable mib-binding

no enable mib-binding

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

The latest standards stipulate that the MIB operation can be performed on a single instance. By default, the MIB operation is performed on the first displayed IS-IS instance. Because multiple IS-IS instances can be configured, the administrator can use this command to specify the instances on which the MIB operation will be performed.

Examples

The following example binds an instance for IS-IS MIB operation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 enable traps

Function

Run the **enable traps** command to enable the trap message sending function of IS-IS.

Run the **no** form of this command to disable this function.

The IS-IS trap message sending function is disabled by default.

Syntax

enable traps { **all** | *traps set* }

no enable traps { **all** | *traps set* }

Parameter Description

all: Indicates all IS-IS trap messages.

traps set: Trap message type in any set.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

IS-IS packets are classified into 18 types and grouped into several sets based on characteristics, with each set containing several trap message types. To send IS-IS trap messages, run the **snmp-server enable traps isis** command to enable the global trap switch of IS-IS, specify a host to receive IS-IS trap messages, and then run this command to specify the types of IS-IS trap messages that can be sent.

Examples

The following example enables the trap message sending function and sets the IP address of the message receiving host to 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable traps isis
Hostname(config)# snmp-server host 10.1.1.1 traps version 2c public
Hostname(config)# router isis
```

```
Hostname(config-router)# enable traps all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 exit-address-family

Function

Run the **exit-address-family** command to exit the IS-IS IPv6 address family configuration mode and go back to the IS-IS routing process configuration mode.

Syntax

exit-address-family

Parameter Description

N/A

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example exits the IS-IS IPv6 address family configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# address-family ipv6 unicast
Hostname(config-router-af)# exit-address-family
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 graceful-restart

Function

Run the **graceful-restart** command to enable the GR capability of IS-IS.

Run the **no** form of this command to disable this capability.

The IS-IS GR capability is enabled by default.

Syntax

graceful-restart

no graceful-restart

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure the IS-IS GR capability. As long as the network conditions remain unchanged, IS-IS can be restarted and restored to the pre-restart state without impact on data forwarding.

Examples

The following example enables the IS-IS GR capability.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis graceful-restart**

1.19 graceful-restart grace-period

Function

Run the **graceful-restart grace-period** command to configure the maximum GR interval of a device.

Run the **no** form of this command to restore the default configuration.

The maximum GR interval is **300** seconds by default.

Syntax

graceful-restart grace-period *max-interval*

no graceful-restart grace-period

Parameter Description

max-interval: Maximum GR interval of a device, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum GR interval of a device to **40** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart grace-period 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 graceful-restart helper disable

Function

Run the **graceful-restart helper disable** command to disable the IS-IS GR Helper capability.

Run the **no** form of this command to enable this capability.

The IS-IS GR Helper function is enabled by default.

Syntax

graceful-restart helper disable

no graceful-restart helper disable

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After you use this command to disable the IS-IS GR Helper capability, IS-IS ignores GR requests of the device.

Examples

The following example disables the IS-IS GR Helper capability.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart helper disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 hello padding

Function

Run the **hello padding** command to enable padding specified IS-IS Hello packets.

Run the **no** form of this command to disable this function.

Padding is enabled for hello packets of the LAN and P2P types by default.

Syntax

hello padding [**multi-point** | **point-to-point**]

no hello padding [**multi-point** | **point-to-point**]

Parameter Description

multi-point: Pads the hello packets of the LAN type.

point-to-point: Pads the hello packets of the P2P type.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

By padding hello packets, IS-IS can advertise neighbors of the MTU supported by the local device. You can use this command to enable or disable padding all hello packets sent by the local IS-IS process. You can also use this command to disable padding all hello packets of the LAN type or P2P type.

The **isis hello padding** command applies to padding in interface configuration mode. To disable padding hello packets on a specified interface, disable padding the packets in IS-IS routing process configuration mode or interface configuration mode.

Examples

The following example disables padding hello packets of the P2P type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# no hello padding point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 hostname dynamic

Function

Run the **hostname dynamic** command to replace the system ID of a device with the host name of the destination device.

Run the **no** form of this command to remove this configuration.

The dynamic host name function is enabled by default.

Syntax

hostname dynamic

no hostname dynamic

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Run this command to replace the system ID of a device with the host name of the destination device. The system IDs that can be displayed by running the **show isis database** and **show isis neighbors** commands are replaced with the host name of the destination device.

Examples

The following example replaces the system ID of a device with the host name of the destination device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# hostname dynamic
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis neighbors**
- **show isis database**

1.23 ignore-lsp-errors

Function

Run the **ignore-lsp-errors** command to ignore LSP checksum errors.

Run the **no** form of this command to remove this configuration.

LSP checksum errors are processed by default.

Syntax

ignore-lsp-errors

no ignore-lsp-errors

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After receiving an LSP, the local IS-IS router calculates its checksum and compares it with the checksum contained in the LSP. If the two checksums are inconsistent, the LSP will be discarded by default. If you run the **ignore-lsp-errors** command to ignore checksum errors, the LSP will be processed normally despite checksum inconsistency.

Examples

The following example configures to ignore LSP checksum errors.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# ignore-lsp-errors
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 interfaces-protocol-compatible

Function

Run the **interfaces-protocol-compatible** command to pad the TLV field of the IS-IS protocol based on protocols supported by an interface.

Run the **no** form of this command to restore the default configuration.

The TLV field of the IS-IS protocol is padded based on protocols supported by an interface by default.

Syntax

interfaces-protocol-compatible

no interfaces-protocol-compatible

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

In single topology mode, a Ruijie device connects to a device of another vendor, a loopback interface is configured on both devices, both IS-IS IPv4 IS-IS and IPv6 IS-IS are enabled, and only a single protocol stack (IPv4 IS-IS or IPv6 IS-IS) is configured on the interconnected interfaces of the two devices. The device of the other vendor sends TLV#129 (supporting only a single protocol stack) based on interfaces whereas Ruijie device sends TLV#129 (supporting dual protocol stacks) based on instances. As a result, the displayed neighbor status on the device of the other vendor is "Init". Ruijie device failed to establish a neighbor relationship with the device of the other vendor. To solve this issue, this command can be configured to enable neighbor relationship establishment between Ruijie devices and devices of other vendors.

Examples

The following example pads the TLV field of the IS-IS protocol based on protocols supported by an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# interfaces-protocol-compatible
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ip router isis

Function

Run the **ip router isis** command to enable the IPv4 IS-IS routing function on an interface.

Run the **no** form of this command to disable this function.

The IPv4 IS-IS routing function is not enabled on an interface by default.

Syntax

ip router isis [*tag*]

no ip router isis [*tag*]

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Note

This command must be run to enable the IS-IS function on an interface in an IPv4 network.

An IS-IS instance named tag runs on an interface. If no such instance exists or will be started and initialized in the name of tag, the IS-IS routing function will not be started on this interface.

Use this command to enable an interface to participate in IS-IS IPv4 routing. Use the **no** form of this command to disable the IS-IS routing process on the interface.

If you run the **no ip routing** command in global configuration mode, IS-IS will disable IPv4 routing on all interfaces. That is, the **no ip router isis** [**tag**] command is automatically executed on all interfaces. Other IS-IS settings remain unchanged.

An instance named tag can be started on 255 broadcast network interfaces at most, whereas, it can be started on unlimited number of P2P network interfaces.

Examples

The following example enables the IPv4 IS-IS routing function on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# ip router isis
```

Notifications

If this interface has been added to another IS-IS instance, the following notification will be displayed:

```
% Interface enabled in another area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip routing** (IP routing/routing management)
- **show isis interface**
- **show isis protocol**

1.26 ipv6 router isis

Function

Run the **ipv6 router isis** command to enable the IPv6 IS-IS routing function on an interface.

Run the **no** form of this command to disable this function.

The IPv6 IS-IS routing function is not enabled on an interface by default.

Syntax

ipv6 router isis [*tag*]

no ipv6 router isis [*tag*]

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

> **Note**
>
> This command must be run to enable the IS-IS function on an interface in an IPv6 network.

After this command is run, an IS-IS instance named tag runs on an interface. If no such instance exists or will be started and initialized in the name of tag, the IPv6 IS-IS routing function will not be started on this interface.

If you run the **no ipv6 unicast-routing** command in global configuration mode, IS-IS will disable IPv6 routing on all interfaces.

An instance named tag can be started on 255 broadcast network interfaces at most, whereas, it can be started on unlimited number of P2P network interfaces.

Examples

The following example enables the IPv6 IS-IS routing function on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# ipv6 router isis
```

Notifications

If this interface has been added to another IS-IS instance, the following notification will be displayed:

```
% Interface enabled in another area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 unicast-routing** (IP routing basics)
- **show isis interface**
- **show isis protocol**

1.27 isis authentication key-chain

Function

Run the **isis authentication key-chain** command to configure a key chain for IS-IS interface authentication.

Run the **no** form of this command to remove this configuration.

The IS-IS interface authentication key chain function is disabled by default.

Syntax

isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

name-of-chain: Name of a key chain. The maximum length is 255.

level-1: Indicates that the authentication key chain takes effect for Level-1.

level-2: Indicates that the authentication key chain takes effect for Level-2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Authentication is not performed if no key chain is configured using the **key chain** command.

(1) If the **authentication mode** command is run with this command, the authentication type configured in the **authentication mode** command is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **authentication mode** command to specify the authentication mode.

(2) If only this command is run, the authentication type specified by the key-chain is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **key chain** command to specify the authentication mode.

For plaintext authentication, the key-string in the key chain cannot exceed 80 characters; otherwise, the key chain will be invalid.

Only one key chain can be used at a time. After you configure a new key chain, it will replace the original one.

If no Level is specified, the key chain takes effect for Level-1 and Level-2.

The key chain is applicable to Hello packets. IS-IS will send or receive passwords that belong to the key chain.

A key chain may contain multiple passwords. A password with a smaller SN is preferentially used for sending a packet. When the packet arrives at the peer device, the device will receive the packet if the packet-carried password is consistent with a password in the key chain.

The authentication commands (for example, **authentication key-chain**) executed in IS-IS routing process configuration mode are intended for LSPs and SNPs. They do not take effect for IS-IS interfaces.

If key chain authentication is configured and the authentication type specified in the key chain is SM3, the range of Algorithm-ID is 0 to 255. If the Algorithm-ID exceeds the range, IS-IS packets do not carry TLV information for authentication. In this case, local authentication and checking will fail.

Examples

The following example specifies the key chain with the name kc for authentication on the IS-IS interface TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
```

```
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication key-chain kc
```

Notifications

N/A

Common Errors

- The key-string in the key chain exceeds 80 characters.

Platform Description

N/A

Related Commands

- **isis authentication mode**

1.28 isis authentication mode

Function

Run the **isis authentication mode** command to enable an authentication mode of an IS-IS interface.

Run the **no** form of this command to disable this mode.

The interface authentication mode is disabled by default.

Syntax

isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

Parameter Description

md5: Specifies the MD5 authentication mode.

text: Specifies the plaintext authentication mode.

level-1: Specifies that the interface authentication mode takes effect for Level-1.

level-2: Specifies that the interface authentication mode takes effect for Level-2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

Run the **authentication mode** command to specify the authentication mode before you can make the key chain configured using the **authentication key-chain** command take effect.

If you use the **isis authentication mode** command after the **isis password** command is executed to configure plaintext authentication, the previous command configuration will be overwritten.

The **isis password** command does not take effect if the **isis authentication mode** command is executed. To run the **isis password** command, delete the **isis authentication mode** command configuration first.

Examples

The following example specifies the Level-2 authentication mode on the IS-IS interface TenGigabitEthernet 0/1 as MD5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication mode md5 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 isis authentication send-only

Function

Run the **isis authentication send-only** command to apply a specified IS-IS interface authentication mode to only sent packets. Received packets are not authenticated.

Run the **no** form of this command to restore the default configuration.

Packets sent and received on an interface are authenticated by default.

Syntax

isis authentication send-only [**level-1** | **level-2**]

no isis authentication send-only [**level-1** | **level-2**]

Parameter Description

level-1: Sets **send-only** for Level-1 on an interface.

level-2: Sets **send-only** for Level-2 on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to enable IS-IS to set an authentication password in the Hello packets sent by an interface. Received packets are not authenticated. You can use this command before you deploy IS-IS interface authentication on all devices in the network or before you change the authentication password or authentication mode. After you run the **isis authentication send-only** command, the devices will not authenticate received Hello packets to avoid network flapping when IS-IS interface authentication is deployed. After authentication is deployed in the entire network, run the **no isis authentication send-only** command to cancel the **send-only** setting.

This command is applicable to plaintext authentication and MD5 authentication. You can run the **isis authentication mode** command to specify the authentication mode for an IS-IS interface.

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2 on the interface.

Examples

The following example specifies that Level-1 authentication applies to only sent packets on the IS-IS interface TenGigabitEthernet 0/1. Received packets are not authenticated.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication send-only level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis database**

1.30 isis bfd

Function

Run the **isis bfd** command to enable IS-IS correlation with BFD on an interface.

Run the **no** form of this command to disable this function.

The IS-IS correlation with BFD function is enabled on an interface by default if the **bfd all-interfaces** command is run. The IS-IS correlation with BFD function is not enabled on an interface if the **bfd all-interfaces** command is not run. The anti-congestion option is disabled by default.

Syntax

isis bfd [**anti-congestion** | **disable**]

no isis bfd [**anti-congestion** | **disable**]

Parameter Description

anti-congestion: Indicates the IS-IS BFD anti-congestion option.

disable: Disables IS-IS correlation with BFD on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can enable or disable BFD on an IS-IS interface by using any of the following two methods:

Method 1: Run the [**no**] **bfd all-interfaces** [**anti-congestion**] command in IS-IS routing process configuration mode to enable or disable BFD on all IS-IS interfaces.

Method 2: Run the **isis bfd** [**disable** | **anti-congestion**] command in interface configuration mode to enable or disable BFD on the specified interface.

Normally, BFD sends detection packets at millisecond intervals to detect the link state. When a link exception (such as a disconnected link) occurs, BFD can quickly detect it and instruct IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Then IS-IS recalculates and generates a new route to bypass the abnormal link, thus realizing fast convergence. With the introduction of new techniques such as the Multi-Service Transport Platform (MSTP), link congestion tends to occur during peak hours of data communication. BFD quickly detects the link exception and instructs IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Link switch is performed to bypass the congested link. A Hello packet for IS-IS neighbor detection is sent every 10s and its expiration time is 30s. The Hello packet can still be received normally when BFD detects an exception, and therefore an IS-IS neighbor relationship is reestablished quickly, causing the route to be restored to the congested link. Then BFD detects the abnormal link and link switch is performed again. This process is repeated, which makes the route be switched between the congested link and other links, causing repetitive flapping.

The anti-congestion option is used to avoid routing flapping in case of link congestion. After the option is configured, the IS-IS neighbor state is still kept alive when link congestion occurs, but the neighbor reachability information in LSPs is deleted. The route is switched to a normal link. When the congested link is restored, the neighbor reachability information in LSPs is recovered and the route is switched back, which avoids route flapping.

When you run the **bfd all-interfaces [anti-congestion]** command, you must run the **bfd up-dampening** command on the interface. The two commands must be used together. If you run only one command, the anti-congestion feature may not take effect or other network exceptions may occur.

Note

- You must configure a BFD session on the interface before you enable IS-IS correlation with BFD.
- When you run the **bfd up-dampening** command on an interface with IS-IS correlation with BFD, you must run the **bfd all-interfaces [anti-congestion]** command.
- When you run the **bfd all-interfaces** command with the **[anti-congestion]** option selected, run the **bfd up-dampening** command on the interface.

Examples

The following example disables IS-IS correlation with BFD on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no switchport
Hostname(config-if-TenGigabitEthernet 0/1)# isis bfd disable
```

The following example enables the IS-IS BFD anti-congestion option on TenGigabitEthernet 0/1 and runs the BFD anti-congestion option.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no switchport
Hostname(config-if-TenGigabitEthernet 0/1)# isis bfd anti-congestion
Hostname(config-if-TenGigabitEthernet 0/1)# bfd up-dampening 60000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis interface**
- **show isis neighbors**
- **show bfd neighbors detail** (reliability/BFD)

1.31 isis circuit-type

Function

Run the **isis circuit-type** command to configure an IS-IS level on an interface.

Run the **no** form of this command to restore the default configuration.

An interface runs on Level-1/Level-2 by default.

Syntax

isis circuit-type { **level-1** | **level-1-2** | **level-2-only** [**external**] }

no isis circuit-type

Parameter Description

level-1: Establishes a Level-1 neighbor relationship.

level-2-only: Establishes a Level-2 neighbor relationship.

level-1-2: Establishes a Level-1/Level-2 neighbor relationship.

external: Uses the interface as an external domain interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If **circuit-type** is set to Level-1 or Level-only, IS-IS will only send PDUs at the corresponding level.

If **is-type** is set to **level-1** or **level-only**, the IS-IS instance only processes transactions at the corresponding level. In this case, the interface only sends the PDUs of the same Level specified by the **is-type** and **circuit-type** commands.

If the interface is set to external, the interface is used as an external domain interface and IS-IS will not send PDUs at the corresponding Level.

Examples

The following example sets the level of TenGigabitEthernet 0/1 to level-2-only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis circuit-type level-2-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 isis csnp-interval

Function

Run the **isis csnp-interval** command to specify the CSNP broadcast interval on an IS-IS interface.

Run the **no** form of this command to restore the default configuration.

CSNPs are sent at an interval of **10** seconds in a broadcast network by default. No CSNPs are sent in a P2P network by default.

Syntax

isis csnp-interval *interval* [**level-1** | **level-2**]

no isis csnp-interval [*interval*] [**level-1** | **level-2**]

Parameter Description

interval: CSNP transmission interval, in seconds. The value range is from 0 to 65535.

level-1: Applies transmission interval only to Level-1 CSNPs.

level-2: Applies transmission interval only to Level-2 CSNPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the CSNP interval. By default, the DIS sends CSNPs every 10s in a broadcast network.

In a P2P network, CSNPs are sent only after a neighbor relationship is established. If an interface is configured as **mesh-groups**, CSNP sending interval can be configured. If **csnp-interval** is set to 0, no CSNP is sent.

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

Examples

The following example sets the CSNP broadcast interval to **20** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis csnp-interval 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 isis hello padding

Function

Run the **isis hello padding** command to enable padding IS-IS hello packets sent on an IS-IS interface.

Run the **no** form of this command to remove this configuration.

Padding is enabled by default for hello packets sent on an interface.

Syntax

isis hello padding

no isis hello padding

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By padding hello packets, IS-IS can advertise neighbors of the MTU supported by the local device.

The **hello padding** command applies to padding in IS-IS routing process configuration mode. To disable padding hello packets on a specified interface, disable padding the packets in IS-IS routing process configuration mode or interface configuration mode.

Examples

The following example disables padding IS-IS hello packets on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no isis hello padding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 isis hello-interval

Function

Run the **isis hello-interval** command to configure the hello packet sending interval on an interface.

Run the **no** form of this command to restore the default configuration.

Hello packet are sent at an interval of **10** seconds by default.

Syntax

isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]

no isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]

Parameter Description

interval: Hello packet sending interval, in seconds. The value range is from 1 to 65535.

minimal: Uses the minimum holdtime **1** second.

level-1: Takes effect for Level-1 Hello packets.

level-2: Takes effect for Level-2 Hello packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

Use this command to modify the Hello packet sending interval. Hello packets are sent at an interval of **10** seconds by default. A DIS sends Hello packets at a frequency three times that by non-DIS devices in a broadcast network. If the local device is elected as the DIS on the interface, this interface sends hello packet every 3.3s by default.

The default hello multiplier of an IS-IS interface is **3**. The holdtime in hello packets is the hello-interval multiplied by this multiplier. If the keyword **minimal** is used, the holdtime in hello packets is set to **1**, the hello packet sending interval is the result of one divided by the hello multiplier. If the hello multiplier is set to **4** and the **isis hello-interval minimal** command is executed, the packet sending interval is **250** ms.

CPU protection is enabled by default. For packets sent to each destination group address (AllISSystems, AllL1ISSystems, and AllL2ISSystems), the number of packets sent to the CPU is limited to 400 per second. If a device has many neighbor relationships or sends Hello packets at short intervals, the IS-IS packets that the device receives may exceed the default limit, causing frequent flapping of neighbor relationships. To solve the problem, you can use the CPU protection command in global configuration mode to increase the limit.

Examples

The following example sets the Level-1 hello packet sending interval to **5** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-interval 5 level-1
```

The following example sets the minimum hello packet holdtime to **1** second on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-interval minimal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 isis hello-multiplier

Function

Run the **isis hello-multiplier** command to configure the multiplier of the hello holdtime on an interface.

Run the **no** form of this command to restore the default configuration.

The default multiplier of the hello holdtime on an interface is **3**.

Syntax

isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]

no isis hello-multiplier [*multiplier-number*] [**level-1** | **level-2**]

Parameter Description

multiplier-number: Multiplier of the hello holdtime on an IS-IS interface. The value range is from 2 to 100.

level-1: Takes effect for Level-1 hello packets.

level-2: Takes effect for Level-2 hello packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The holdtime in hello packets is equal to the hello-interval multiplied by the hello multiplier.

Examples

The following example sets the multiplier of the hello holdtime to **5** on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-multiplier 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 isis lsp-flood

Function

Run the **isis lsp-flood** command to configure the maximum number of LSP packets sent by the IS-IS interface at a time.

Run the **no** form of this command to restore the default configuration.

An interface can send a maximum of 5 LSP packets at a time by default.

Syntax

isis lsp-flood *lsp-number* [**level-1** | **level-2**]

no isis lsp-flood [**level-1** | **level-2**]

Parameter Description

lsp-number: Maximum number of LSP packets sent by the IS-IS interface at a time. The value range is from 1 to 1000.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of Level-2 LSP packets sent by TenGigabitEthernet 0/1 at a time to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis lsp-flood 10 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 isis lsp-interval

Function

Run the **isis lsp-interval** command to configure the LSP sending interval on an interface.

Run the **no** form of this command to restore the default configuration.

LSPs are sent at an interval of **33** ms by default on an IS-IS interface.

Syntax

isis lsp-interval *pdu-interval* [**level-1** | **level-2**]

no isis lsp-interval [**level-1** | **level-2**]

Parameter Description

pdu-interval: LSP sending interval, in milliseconds. The value range is from 1 to 4294967295.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

Examples

The following example sets the Level-2 LSP sending interval to **100** ms on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis lsp-interval 100 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 isis mesh-group

Function

Run the **isis mesh-group** command to add an IS-IS interface to a specified mesh group.

Run the **no** form of this command to remove this configuration.

No interface joins any mesh group by default.

Syntax

isis mesh-group { **blocked** | *mesh-group-id* }

no isis mesh-group

Parameter Description

blocked: Blocks all LSP forwarding on this interface.

mesh-group-id: ID of a mesh group an interface joins. The value range is from 1 to 4294967295.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Mesh-groups can control transitional and redundant LSPs in an NBMA network. In normal cases, an IS-IS device advertises LSPs from all other interfaces except the packet receiving interface. If a device is configured with multiple interfaces, LSPs will be sent from all these interfaces. In this case, neighbors will receive duplicate LSPs. This wastes a huge amount of CPU and bandwidth resources.

The IS-IS mesh group allows a device to group interfaces. If an LSP is received by any interface in a group, this LSP will not be advertised by other interfaces in the group. If the LSP is received from an interface out of the group, the LSP will be advertised from other interfaces as usual.

When you need to set **mesh-group** on an IS-IS interface, run the **isis csnp-interval** command to configure the non-0 CSNP sending interval to ensure complete LSP synchronization between neighbors in the network. After that, CNSPs will be periodically sent to synchronize LSPs.

Examples

The following example adds the IS-IS interface TenGigabitEthernet 0/1 to a specified mesh group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis mesh-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 isis metric

Function

Run the **isis metric** command to configure the metric for an IS-IS interface.

Run the **no** form of this command to configure the metric for an IS-IS interface as a default value.

Level-1 and Level-2 use the computation result of **bandwidth-reference** by default.

Syntax

isis metric *metric* [**level-1** | **level-2**]

no isis metric [*metric*] [**level-1** | **level-2**]

Parameter Description

metric: Metric value. The value range is from 1 to 63.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The metric value, which is used in IP calculation, is stored in the TLV of the IP reachability information. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation.

The metric belongs to the narrow type and is valid only when **metric-style** is set to Narrow.

Examples

The following example sets the metric on the IS-IS interface TenGigabitEthernet 0/1 to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis metric 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **metric-style**

1.40 isis network point-to-point

Function

Run the **isis network point-to-point** command to change the type of an interface from broadcast to P2P.

Run the **no** form of this command to restore the default configuration.

The default type of an interface is broadcast.

Syntax

isis network point-to-point

no isis network [**point-to-point**]

Parameter Description

point-to-point: Configures an interface as a P2P interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the type of an interface from broadcast to P2P. This command is valid to broadcast network interfaces.

If the current interfaces have been configured with the IS-IS protocol and the number of broadcast network interfaces configured with the same IS-IS protocol reaches 255 (for example, **ip router isis** [**tag**] or **ipv6 router isis** [**tag**] is configured, or the interfaces are passive interfaces), this configuration cannot be deleted.

Examples

The following example changes the interface type of TenGigabitEthernet 0/1 from broadcast to P2P.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis network point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis interface**

1.41 isis passive

Function

Run the **isis passive** command to configure an interface as a passive interface.

Run the **no** form of this command to remove this configuration.

The configured passive interface in the IS-IS routing process configuration mode prevails by default.

Syntax

isis passive

no isis passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command prevents the interface from receiving or sending IS-IS packets, but the IP address of this interface is flooded through other interfaces. The command is valid only for the generated IS-IS interface.

Examples

The following examples configures TenGigabitEthernet 0/1 as a passive interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis passive
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis interface**

1.42 isis password

Function

Run the **isis password** command to configure the password for plaintext authentication of hello packets on an interface.

Run the **no** form of this command to remove this configuration.

Syntax

isis password [**0** | **7**] *password-string* [**send-only**] [**level-1** | **level-2**]

no isis password [**send-only**] [**level-1** | **level-2**]

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent packets. Received packets are not authenticated.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Use this command to configure the password for Hello packet authentication on an interface. Use the **no** form of this command to clear the password.

If no Level is specified by default, the password takes effect for Level-1 and Level-2 circuit types.

This command does not take effect if the **isis authentication mode** command is executed. You need to first delete the previous command configuration.

If you include the **send-only** parameter when deleting the **isis authentication mode** command configuration, only the parameter setting is canceled.

Examples

The following example sets the password for plaintext authentication of hello packets to **redgiant** on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis password redgiant
```

Notifications

If authentication is configured using the **isis authentication mode** command, the following notification will be displayed:

```
% Please configure password using isis authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 isis priority

Function

Run the **isis priority** command to configure the priority for DIS election in a LAN.

Run the **no** form of this command to restore the default configuration.

The default priority of a device for Level-1 and Level-2 DIS election is **64**.

Syntax

isis priority *value* [**level-1** | **level-2**]

no isis priority [*value*] [**level-1** | **level-2**]

Parameter Description

value: Priority for DIS election in a LAN. The value range is from 0 to 127.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the priority in Hello packets in a LAN.

A lower DIS priority of an interface indicates a lower priority of being elected as a DIS.

This command is invalid on a P2P network interface.

The **no isis priority** command, with or without parameters, restores the priority to its default value. To change the configured priority, run the **isis priority** command with the priority specified to overwrite the existing configuration, or you can first restore the priority to its default value and then configure a new priority.

Examples

The following example sets the priority for Level-1 DIS election on TenGigabitEthernet 0/1 to 127.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis priority 127 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis interface**

1.44 isis psnp-interval

Function

Run the **isis psnp-interval** command to configure the minimum PSNP sending interval.

Run the **no** form of this command to remove this configuration.

The function of configuring the PSNP sending interval is disabled by default. In this case, the default minimum PSNP sending interval is **2** seconds and it takes effect for Level-1 and Level-2 PSNPs.

Syntax

isis psnp-interval *psnp-interval* [**level-1** | **level-2**]

no isis psnp-interval [**level-1** | **level-2**]

Parameter Description

psnp-interval: PSNP interval, in seconds. The value range is from 1 to 120.

level-1: Takes effect for Level-1 PSNPs.

level-2: Takes effect for Level-2 PSNPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

PSNPs are mainly used to request LSPs that are absent locally or respond to received LSPs (in a P2P network). The PSNP interval should be minimized. If many LSPs exist and the device performance is low, you can increase the PSNP sending interval and LSP retransmission interval to reduce the device load.

Examples

The following example sets the Level-2 PSNP sending interval to 5 seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis psnp-interval 5 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 isis retransmit-interval

Function

Run the **isis retransmit-interval** command to configure the LSP retransmission interval on an IS-IS interface.

Run the **no** form of this command to restore the default configuration.

The default LSP Retransmit-interval is **5** seconds, and it takes effect for Level-1 and Level-2 LSPs.

Syntax

isis retransmit-interval *retransmit-interval* [**level-1** | **level-2**]

no isis retransmit-interval [**level-1** | **level-2**]

Parameter Description

retransmit-interval: Retransmission interval, in seconds. The value range is from 0 to 65535.
level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

Use this command to configure the LSP retransmission interval. In a P2P network, after a device sends an LSP, if the device receives no PSNP response within the time specified by retransmit-interval, it will resend the LSP. If the retransmission interval is set to **0**, the LSP will not be resent.

Examples

The following example sets the Level-2 LSP sending interval to **10** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis retransmit-interval 10 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 isis subvlan

Function

Run the **isis subvlan** command to enable the IS-IS function in a super VLAN.

Run the **no** form of this command to restore the default configuration.

The IS-IS function takes effect in super VLAN only and is disabled by default.

Syntax

isis subvlan [**all** | *vlan-id*]

no isis subvlan

Parameter Description

all: Allows sending packets to all sub VLANs

vlan-id: Sub VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, which exceeds the processing capability of the device. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the IS-IS function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the IS-IS function must be run on the super VLAN, but packets need to be sent to only one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. You can use this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the IS-IS function on super VLAN 300 and allows sending packets to sub VLAN 1024.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# isis subvlan 1024
```

Notifications

N/A

Common Errors

- The function is configured on a non-super VLAN.
- The specified sub VLAN on the super VLAN cannot implement interworking with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.47 isis suppress on-neighbor-up

Function

Run the **isis suppress on-neighbor-up** command to suppress routing calculation after an IS-IS neighbor is up.

Run the **no** form of this command to remove this configuration.

The route calculation suppression function is disabled by default.

Syntax

isis suppress on-neighbor-up *delay-time*

no isis suppress on-neighbor-up

Parameter Description

delay-time: Delay time of suppressing route calculation, in seconds. The value range is from 1 to 60.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the interface neighbor is up, this command prevents the neighbor reachability information from being added to LSP so as to delay the routing calculation. When the timer expires, the neighbor reachability information is added to LSP to start the routing calculation. This function prevents the route calculation from using the old LSP, which may lead to route flapping.

Examples

The following example suppresses route calculation after the IS-IS neighbor on TenGigabitEthernet 0/1 is up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis suppress on-neighbor-up 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP routing basic)

1.48 isis three-way-handshake disable

Function

Run the **isis three-way-handshake disable** command to disable three-way handshake of a P2P network.

Run the **no** form of this command to enable three-way handshake of a P2P network.

Three-way handshake is performed in a P2P network by default.

Syntax

isis three-way-handshake disable

no isis three-way-handshake disable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Neighbor establishment in a P2P network requires three-way handshake. The neighbor relationship can be established only after the three-way handshake succeeds. If you want to accelerate neighbor establishment or there is device that does not support three-way handshake, you can run this command to cancel three-way handshake.

Examples

The following example disables three-way handshake on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis network point-to-point
Hostname(config-if-TenGigabitEthernet 0/1)# isis three-way-handshake disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 isis wide-metric

Function

Run the **isis wide-metric** command to configure the wide metric value for an interface.

Run the **no** form of this command to configure the wide metric value of an interface as a default value.

The default wide metric value of Level-1 and Level-2 is the computation result of **bandwidth-reference**.

Syntax

isis wide-metric *metric* [**level-1** | **level-2**]

no isis wide-metric [*metric*] [**level-1** | **level-2**]

Parameter Description

metric: Metric value. The value range is from 1 to 16777214, and the default value is the computation result of **bandwidth-reference**.

level-1: Takes effect for the Level-1 links.

level-2: Takes effect for the Level-2 links.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The metric value, which is used in IP calculation, is stored in the TLV of the IP reachability information. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation.

The metric is valid only when **metric-style** is set to **Wide**.

Examples

The following example sets the wide metric value of TenGigabitEthernet 0/1 to **1000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis wide-metric 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **metric-style**

1.50 is-name

Function

Run the **is-name** command to replace the system ID of an instance with the configured name.

Run the **no** form of this command to remove this configuration.

The name customization function is disabled by default.

Syntax

is-name *name*

no is-name

Parameter Description

name: Alias of an instance, which is a string of a maximum of 64 characters.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to replace the system ID of an instance with the configured name. The system IDs that can be displayed by running the **show isis database** and **show isis neighbors** commands are replaced with the configured name.

Examples

The following example replaces the system ID of an instance with dut.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# is-name dut
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis neighbors**
- **show isis database**

1.51 is-type

Function

Run the **is-type** command to specify the level at which IS-IS runs.

Run the **no** form of this command to restore the default configuration.

IS-IS runs at Level-1/Level-2 by default.

Syntax

is-type { **level-1** | **level-1-2** | **level-2-only** }

no is-type

Parameter Description

level-1: Indicates that IS-IS only runs at Level-1.

level-1-2: Indicates that IS-IS runs at Level-1 and Level-2.

level-2-only: Indicates that IS-IS only runs at Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Changing the IS-IS type will enable or disable the routes of the corresponding level.

Examples

The following example enables IS-IS to only run at Level-1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# is-type level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 log-adjacency-changes

Function

Run the **log-adjacency-changes** command to record neighbor state changes of IS-IS without enabling the **debug** command.

Run the **no** form of this command to disable this function.

The function of recording neighbor state changes of IS-IS is enabled by default without the **debug** command.

Syntax

log-adjacency-changes

no log-adjacency-changes

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Using the **debug** command to record neighbor state changes of IS-IS will consume a great amount of system resources. Run this command to record neighbor state changes of IS-IS without enabling the **debug** command.

Examples

The following example records neighbor state changes of IS-IS without enabling the **debug** command.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# log-adjacency-changes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 lsp-fragments-extend

Function

Run the **lsp-fragments-extend** command to enable fragment extension.

Run the **no** form of this command to disable this function.

The fragment extension function is disabled by default.

Syntax

lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]

no lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]

Parameter Description

level-1: Enables LSP fragment extension on Level-1.

level-2: Enables LSP fragment extension on Level-2.

compatible: Indicates compatibility with the RFC version of extended LSPs.

rfc3786: Indicates the old version of extended LSPs.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

There are up to 256 LSP fragments. When the fragments are used up, subsequent link state information, including neighbor information and IP route information, will be discarded, causing a network exception.

To solve this problem, enable fragment extension at the specified level and configure an additional system ID by using the **virtual-system** command.

When you enable or disable the **compatible** option for a network containing RFC 3786 compliant devices of other vendors, observe the LSDB of the related devices. If there are LSPs affecting network routing existing in the network, run the **clear isis *** command to clear the LSPs and trigger LSDB synchronization.

Examples

The following example enables fragment extension on Level-2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-fragments-extend level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 lsp-gen-interval

Function

Run the **lsp-gen-interval** command to configure an exponential backoff algorithm of LSP generation.

Run the **no** form of this command to restore the default configuration.

The default maximum interval of two LSP generations is **5** seconds, the delay of LSP generation is **50** ms, and the maximum interval for the first and second LSP generations is **200** ms. The configuration takes effect for Level-1 and Level-2 LSPs.

Syntax

lsp-gen-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

no lsp-gen-interval [**level-1** | **level-2**]

Parameter Description

level-1: Takes effect for Level-1 IS-IS LSPs.

level-2: Takes effect for Level-2 IS-IS LSPs.

maximum-interval: Maximum interval for generating two consecutive LSPs, in seconds. The value range is from 1 to 65535.

initial-interval: Delay for generating LSPs for the first time, in milliseconds. The value range is 0 to 60000.

hold-interval: Minimum interval for the first and second LSP generations, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

The LSP packet generation interval refers to the interval for generating two different LSP packets. A smaller generation interval indicates faster network convergence, which, however, will be accompanied by frequent flooding in the network.

The wait time for generating an LSP packet for the first time is the *initial-interval*. If the network becomes unstable, the LSP packet regeneration interval changes to be less than the *maximum-interval*, and the interval for generating an LSP packet for the second time changes to *hold-interval*. A corresponding penalty will be added to this interval: The next interval for regenerating an LSP packet doubles the previous interval for generating the same LSP packet, until the regeneration interval reaches the *maximum-interval*. Subsequent LSP packets will be generated at the *maximum-interval*. When the network becomes stable, the LSP packet regeneration interval becomes greater than the *maximum-interval*, and the wait time for LSP packet generation is restored to the *initial interval*.

Link changes have high requirements for convergence. The *initial-interval* can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.

Examples

The following example configures an exponential backoff algorithm of LSP generation, and sets the maximum interval of two LSP generations to **10** seconds, the wait time of LSP generation for the first time to **100** ms, and the interval for the first and second LSP generations to **200** ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-gen-interval 10 100 200
```

The following example configures an exponential backoff algorithm of LSP generation, sets the maximum interval of two LSP generations to **5** seconds, and uses the default values of other exponential backoff parameters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-gen-interval 5
```

Notifications

If the configured value of *hold-interval* is greater than *maximum-interval* (for example, the configured value of *hold-interval* is **1500** ms, and the *maximum-interval* is **1** second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than maximum_interval (1s), set to
(1000ms).
```

If the configured value of *initial-interval* is greater than *hold-interval* (for example, the configured value of *initial-interval* is **20** ms, and the *hold-interval* is **10** ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set to
(10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 lsp-length originate

Function

Run the **lsp-length originate** command to configure the maximum length of sent LSPs.

Run the **no** form of this command to restore the default configuration.

The default maximum length of sent LSPs is **1492** bytes, and it takes effect for Level-1 and Level-2 LSPs.

Syntax

lsp-length originate *size* [**level-1** | **level-2**]

no lsp-length originate [**level-1** | **level-2**]

Parameter Description

size: Maximum length of sent LSPs, in bytes. The value range is from 512 to 16000.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

In principle, the maximum length of LSPs and SNPs cannot be greater than the interface MTU; otherwise, the packets will be discarded when being sent.

Examples

The following example sets the maximum length of sent LSPs on Level-2 to **1498** bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis1
Hostname(config-router)# lsp-length originate 1498 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 lsp-length receive

Function

Run the **lsp-length receive** command to configure the maximum length of received LSPs.

Run the **no** form of this command to restore the default configuration.

The default maximum length of received LSPs is **1492** bytes.

Syntax

lsp-length receive *size*

no lsp-length receive

Parameter Description

size: Maximum length of received LSPs, in bytes. The value range is from 1492 to 16000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to control the maximum length of LSPs received by the local device. Intermediate nodes with sufficient memory are required to receive LSPs whose maximum length is equal to the interface MTU in order to avoid a route convergence failure. From this perspective, the command is meaningless. The maximum length of received LSPs cannot be smaller than that of sent LSPs; otherwise, the former will be automatically adjusted to be equal to the latter.

Examples

The following example sets the maximum length of received LSPs to **1498** bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-length receive 1498
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 lsp-refresh-interval

Function

Run the **lsp-refresh-interval** command to configure the LSP refresh interval.

Run the **no** form of this command to restore the default configuration.

The default LSP refresh interval is **900** seconds.

Syntax

lsp-refresh-interval *interval*

no lsp-refresh-interval

Parameter Description

interval: LSP refresh interval, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After an LSP has remained stable for the time specified by this command, it will be refreshed and then advertised.

The LSP refresh interval must be at least 300 seconds less than the maximum LSP lifetime. If the difference of the configured LSP lifetime *max-lifetime* from the LSP refresh interval *interval* is less than 300s, the value of *max-lifetime* minus 300s is used as the LSP refresh interval.

Examples

The following example sets the LSP refresh interval to **600** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-refresh-interval 600
```

Notifications

If the difference of the configured LSP lifetime from the LSP refresh interval is less than 300s, for example, the maximum LSP lifetime is 1000 and the LSP refresh interval is 900, the following notification will be displayed:

```
% ISIS: max-lsp-lifetime should be 300s greater than lsp-refresh-interval
% ISIS: set lsp-refresh-interval to 700s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 max-area-addresses

Function

Run the **max-area-addresses** command to configure the maximum number of area addresses.

Run the **no** form of this command to restore the default configuration.

The default maximum number of area addresses is **3**.

Syntax

max-area-addresses *max-area- number*

no max-area-addresses

Parameter Description

max-area- number: Maximum number of area addresses. The value range is from 3 to 6.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Generally, an IS-IS process is configured with a Network Entry Title (NET) address. During area reallocation, an IS-IS process can be configured with multiple NET addresses to ensure routing correctness. The system ID of multiple NET addresses must be the same. For Level-1 IS-IS devices, neighbor relationship can be created between the routers only when the maximum numbers of area addresses are the same.

Examples

The following example sets the maximum number of area addresses to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-area-addresses 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 maximum-paths

Function

Run the **maximum-paths** command to configure the maximum number of IS-IS equal-cost paths to be added to a routing table.

Run the **no** form of this command to restore the default configuration.

The default maximum number of equal-cost paths is **2**.

Syntax

maximum-paths *maximum*

no maximum-paths

Parameter Description

maximum: Maximum number of IS-IS equal-cost routes to be added to a routing table. The value range is from 1 to 32.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

This command is used by IS-IS to control the number of IS-IS equal-cost paths to be added to a routing table. The routing table also has a command used to control the number of equal-cost paths. The number of effective equal-cost paths is determined by either of the two command values, whichever is smaller.

Examples

The following example sets the maximum number of IS-IS IPv4 equal-cost routes to be added to a routing table to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# maximum-paths 5
```

The following example sets the maximum number of IS-IS IPv6 equal-cost routes to be added to a routing table to **6**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# maximum-paths 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 max-lsp-lifetime

Function

Run the **max-lsp-lifetime** command to configure the maximum LSP lifetime.

Run the **no** form of this command to restore the default configuration.

The default maximum LSP lifetime is **1200** seconds.

Syntax

max-lsp-lifetime *max-lifetime*

no max-lsp-lifetime

Parameter Description

max-lifetime: Maximum LSP lifetime, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

The maximum LSP lifetime must be at least 300s greater than the LSP refresh interval. If the difference of the configured LSP lifetime *max-lifetime* from the LSP refresh interval *interval* is less than 300s, the value of *max-lifetime* minus 300s is used as the LSP refresh interval.

Examples

The following example sets the maximum LSP lifetime to **1200** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-lsp-lifetime 1200
```

Notifications

If the difference of the configured maximum LSP lifetime from the LSP refresh interval is less than 300s, for example, the maximum LSP lifetime is 1000 and the LSP refresh interval is 900, the following notification will be displayed:

```
% ISIS: max-lsp-lifetime should be 300s greater than lsp-refresh-interval
% ISIS: set lsp-refresh-interval to 700s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 max-metric on-neighbor-up

Function

Run the **max-metric on-neighbor-up** command to configure the maximum metric for the directly-connected routes after the first neighbor is up.

Run the **no** form of this command to remove this configuration.

The metric of the directly-connected route is not modified by default after the first neighbor is up.

Syntax

max-metric on-neighbor-up *delay-time*

no max-metric on-neighbor-up

Parameter Description

delay-time: Delay for configuring the maximum metric for the directly-connected routes after the first neighbor is up, in seconds. The value range is from 5 to 1800.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

In the Overlay scene where IS-IS is applied to Underlay, the Overlay tunnel may rely on Underlay routing. After the IS-IS neighbor is up, the Underlay routing is reachable but the Overlay tunnel may not be created, which

may lead to traffic interruption. In this case, run this command to prevent traffic interruption. According to the metric type, the maximum metric for Narrow is 63 and for Wide is 16777214.

Examples

The following example sets the delay for configuring the maximum metric for the directly-connected routes to **100** seconds after the first neighbor is up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-metric on-neighbor-up 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 metric-style

Function

Run the **metric-style** command to configure a metric type.

Run the **no** form of this command to restore the default configuration.

The narrow metric type is used by default.

Syntax

metric-style { **narrow** | **wide** } [**transition**] [**level-1** | **level-1-2** | **level-2**]

no metric-style { **narrow** | **wide** } [**transition**] [**level-1** | **level-1-2** | **level-2**]

Parameter Description

narrow: Uses the narrow metric type. The value range of interface metrics is from 1 to 63.

wide: Uses the wide metric type. The value range of interface metrics is from 1 to 16777214.

transition: Allows a device to send and receive narrow and wide metric types.

level-1: Takes effect for Level-1 interface.

level-1-2: Takes effect for Level-1 and Level-2 interfaces.

level-2: Takes effect for Level-2 interface.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

When the metric type is Narrow, run the **isis metric** command to configure metric values of an interface.

When the metric type is Wide or Transition, run the **isis wide-metric** command to configure metric values of an interface.

Examples

The following example configures the metric type as Wide.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# metric-style wide
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **isis metric**
- **isis wide-metric**

1.63 min-lsp-arrival

Function

Run the **min-lsp-arrival** command to configure the delay for receiving duplicate LSPs.

Run the **no** form of this command to remove this configuration.

The function of delaying receiving duplicate LSPs packets is not supported on Level-1 and Level-2 by default.

Syntax

min-lsp-arrival [**level-1** | **level-2**] *minimum-interval initial-interval hold-interval*

no min-lsp-arrival [**level-1** | **level-2**]

Parameter Description

level-1: Takes effect for Level-1 IS-IS LSPs.

level-2: Takes effect for Level-2 IS-IS LSPs.

minimum-interval: Minimum interval for receiving two duplicate LSP packets, in seconds. The value range is from 1 to 120.

initial-interval: Interval for receiving duplicate LSP packets for the first time, in milliseconds. The value range is 0 to 60000.

hold-interval: Minimum interval for receiving duplicate LSP packets for the first and second times, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

The interval for receiving duplicate LSP packets for the first time is the *initial-interval*. When the interval for receiving duplicate LSP packets is less than the *minimum-interval*, the interval for receiving duplicate LSP packets for the second time becomes the *hold-interval*. In addition, a corresponding penalty is added to this interval: The next interval for receiving duplicate LSP packets doubles the previous interval for receiving the same LSP packets, until this interval reaches the *minimum-interval*. The interval for receiving duplicate LSP packets is changed to *minimum-interval*. When the network becomes stable, the interval for receiving duplicate LSP packets becomes greater than the *minimum-interval*, and the delay for receiving duplicate LSP packets is restored to the *initial-interval*.

Link changes have high requirements for convergence. The *initial-interval* can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- The value of the configured *hold-interval* cannot be greater than that of *minimum-interval*. Otherwise, the value of *hold-interval* is changed to that of *minimum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.

Examples

The following example sets the minimum interval of receiving duplicate LSP packets to **10** seconds, the interval of receiving duplicate LSP packets for the first time to **100** ms, and the interval of receiving duplicate LSP packets for the first and second times to **200** ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# min-lsp-arrival 10 100 200
```

Notifications

If the configured value of *hold-interval* is greater than the *minimum-interval* (for example, the configured value of *hold-interval* is 1500 ms, and the *minimum-interval* is 1 second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than minimum_interval (1s), set to
(1000ms).
```

If the configured value of *initial-interval* is greater than the *hold-interval* (for example, the configured value of *initial-interval* is 20 ms, and the *hold-interval* is 10 ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set to
(10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 multi-topology

Function

Run the **multi-topology** command to configure IS-IS to support IPv6 unicast topologies. After that, IPv4 and IPv6 unicast routes in IS-IS will be calculated based on different topologies.

Run the **no** form of this command to restore the default configuration.

IS-IS does not support IPv6 unicast topologies by default.

Syntax

multi-topology [**transition**]

no multi-topology [**transition**]

Parameter Description

transition: Configures the MT mode, which supports smooth migration from an IPv4/IPv6 hybrid topology to separate IPv4 and IPv6 topologies.

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

The configuration of this command is applied in the following scenarios:

- If this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology. This is a default topology.
- If this command is configured without the **transition** parameter, the router runs in MT mode, and IS-IS IPv4 runs in the default topology and IS-IS IPv6 runs in the IPv6 unicast topology.

- If this command is configured with the **transition** parameter, the router runs in MTT mode, and IS-IS IPv6 runs in the default topology and the IPv6 unicast topology.

The routers in MTT mode can **transfer** the MT TLV or the default topology TLV. The MTT mode is applicable to incremental deployment to ensure smooth network migration. The MTT mode can cause route leaking between the default topology and IPv6 unicast topology. If the MTT mode is configured improperly, network failures such as routing black holes and loops may occur.

The metric type must be set to Wide or Transition before you run this command. The MTR feature will be disabled if the metric type is set to Narrow or only one Level is configured to support the Wide or Transition mode.

Examples

The following example configures IS-IS to support IPv6 unicast topologies.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# multi-topology
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **address-family ipv6**
- **metric-style**

1.65 net

Function

Run the **net** command to configure a NET address in IS-IS.

Run the **no** form of this command to remove this configuration.

No NET address is configured in IS-IS by default.

Syntax

net *net-address*

no net *net-address*

Parameter Description

net-address: NET address, in the format of XX.XXXX.YYYY.YYYY.YYYY.00. In this format, XX.XXXX indicates the area ID and YYYY.YYYY.YYYY indicates the system ID.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure an area ID and a system ID in IS-IS.

Different NET addresses must have the same system ID.

Examples

The following example sets the NET address of IS-IS to 49.0000.0001.0002.0003.00.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# net 49.0000.0001.0002.0003.00
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 nsr

Function

Run the **nsr** command to enable the NSR function for current IS-IS instance.

Run the **no** form of this command to restore the default configuration.

The NSR function is disabled by default.

Syntax

nsr

no nsr

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

NSR backs up relevant IS-IS information from the master Supervisor Engine to the slave Supervisor Engine of the distributed device, or from the master device to the salve device in VSU mode, so that the device can automatically recover the link state and regenerate a route upon active/standby switchover, without requiring help from neighbor devices during the recovery. Information that should be backed up includes the neighbor relationship and link state.

For the same IS-IS process, either NSP or GR is enabled, because they are exclusive.

The switchover of distributed devices and VSU devices takes a period of time. If the IS-IS neighbor keepalive duration is less than the switchover duration, IS-IS neighbor relationship with the neighbor device is removed, and the services are interrupted during the switchover. Therefore, it is recommended that the IS-IS neighbor keepalive duration be set not less than the default value. When Fast Hello is enabled, the IS-IS neighbor keepalive duration is less than 1 second and the IS-IS neighbor relationship times out during the switchover, causing NSR failures. Therefore, it is recommended that Fast Hello be disabled when NSR is enabled.

Examples

The following example enables the NSR function for current IS-IS instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# nsr
```

Notifications

N/A

Common Errors

- If the neighbor keepalive duration is short, when fast hello is enabled, IS-IS neighbor relationship is disconnected during a switchover, causing forwarding interruption.

Platform Description

N/A

Related Commands

- **show isis protocol**
- **show isis nsr**

1.67 passive-interface

Function

Run the **passive-interface** command to configure a passive interface.

Run the **no** form of this command to restore the default configuration.

The passive interface function is not enabled by default.

Syntax

passive-interface { **default** | *interface-type interface-number* }

no passive-interface { **default** | *interface-type interface-number* }

Parameter Description

default: Configures all IS-IS interfaces that are not enabled as passive interfaces.

interface-type: Interface type.

interface-number: Interface number.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

This function prevents the specified interface from receiving and sending IS-IS packets, but the IP address of this interface will be flooded by other interfaces. If the number of interfaces with IS-IS not enabled exceeds 255, only the first 255 interfaces will be configured as passive interfaces. The remaining interfaces are non-passive interfaces.

Examples

The following examples configures TenGigabitEthernet 0/1 as a passive interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# passive-interface tenGigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 redistribute

Function

Run the **redistribute** command to redistribute other routes to IS-IS.

Run the **no** form of this command to remove this configuration.

Redistribution is disabled by default.

Syntax

redistribute { **bgp** | **connected** | **ospf** *process-id* [**match** { **externa**l [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [[**level-1** | **level-1-2** | **level-2**] | **metric** *metric-value* | **metric-type** { **external** | **internal** } | **route-map** *route-map-name*] *

no redistribute { **bgp** | **connected** | **ospf** *process-id* [**match** { **externa**l [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [[**level-1** | **level-1-2** | **level-2**] | **metric** *metric-value* | **metric-type** { **external** | **internal** } | **route-map** *route-map-name*] *

Parameter Description

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

ospf *process-id*: Performs redistribution from OSPF. *process-id* specifies an OSPF process. The value range is from 1 to 65535 and the default value is **1**.

match { **externa**l [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *: Filters route sub-types of OSPF during OSPF route redistribution. If the **match** parameter is not included, all route sub-types of OSPF are received. If **1** or **2** is not specified after **match external**, OSPF routes of **external 1** and **external 2** are redistributed. If **1** or **2** is not specified after **match nssa-external**, OSPF routes of **nssa-external 1** and **nssa-external 2** are redistributed.

match: Redistributes specific OSPFv3 routes that meet the filtering conditions.

external [**1** | **2**]: Redistributes E1, E2, or all external routes.

internal: Redistributes internal routes and inter-area routes.

nssa-external [**1** | **2**]: Redistributes N1, N2, or all external routes of all NSSAs.

rip: Indicates redistribution from RIP.

static: Indicates redistribution from static routes.

level-1 | **level-1-2** | **level-2**: Indicates the Level of redistributed routes received by IS-IS. If no Level is specified, routes are redistributed to Level-2.

level-1: Redistributes routes to Level-1.

level-1-2: Redistributes routes to Level-1 and Level-2.

level-2: Redistributes routes to Level-2.

metric *metric-value*: Sets the metric of a redistributed route. The value range is from 0 to 4261412864. The metric of external routes is used when the **metric** option is not specified.

metric-type { external | internal }: Indicates the metric type of redistributed routes. If no metric type is specified, the metric belongs to the **internal** type.

external: Indicates that the metric belongs to the external type.

internal: Indicates that the metric belongs to the internal type.

route-map *route-map-name*: Indicates the route map used for external route redistribution. It is used to filter redistributed routes or configure the attributes of the redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

Run the **no redistritbue** { **bgp** | **connected** | **ospf** *processs-id* | **rip** | **static** } command to cancel the redistribution of routes mapped to the specified protocol. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution. For example: **no redistribute bgp** cancels BGP route redistribution, whereas **no redistribute bgp route-map aa** cancels the route map named **aa** associated with BGP route redistribution.

When external routes are redistributed in IPv4 mode, the routing information is stored in LSPs' IP External Reachability Information TLV.

When external routes are redistributed in IPv6 mode, the routing information is stored in LSPs' IPv6 Reachable TLV.

In the old versions of some vendors, if the metric type is set to **external**, the metric of redistributed routes is added by 64 during route calculation and routes are selected based on the metric. This practice does not comply with the related protocol. In the actual application, external routes may be preferred over internal routes. If this happens during interworking with old versions of some vendors, you can modify the related setting (such as metric value or metric type) of each device to ensure that internal routes are preferred over external routes.

Examples

The following example redistributes static routes to Level-1 of the current instance and sets the metric value to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# redistribute static metric 10 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis protocol**

1.69 redistribute isis level-1 into level-2

Function

Run the **redistribute isis level-1 into level-2** command to redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

Run the **no** form of this command to remove this configuration.

All Level-1 routes will be automatically redistributed to Level-2 by default.

Syntax

redistribute isis [*tag*] **level-1 into level-2** [**distribute-list** *acl-name* | **route-map** *route-map-name*]

no redistribute isis [*tag*] **level-1 into level-2** [**distribute-list** *acl-name* | **route-map** *route-map-name*]

Parameter Description

tag: Name of the IS-IS instance whose routing information will be redistributed. **distribute-list** *acl-name*: Filters redistributed routes by using **distribute-list**. *acl-name* indicates the associated prefix list, which can be a standard, an extended, or a name prefix list. The format is as follows:

{ *<1-99>* | *<100-199>* | *<1300-1999>* | *<2000-2699>* | *acl-name* }

In IS-IS IPv6 address family configuration mode, only the name prefix list can be used, in the format of *acl-name*.

route-map *route-map-name*: Indicates the route map used for route redistribution. It is used to filter redistributed routes or configure the attributes of redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

You can use the **route-map** or **distribute-list** parameter to filter the specified instance's Level-1 routes to be redistributed. Only the routes that meet specific criteria can be redistributed to Level-2 of the current instance. The **route-map** and **distribute-list** parameters cannot be used at the same time.

The **no redistritbue isis** [*tag*] **level-2 into level-1** command is used to cancel the redistribution of the specified instance's routes. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution.

For example, **no redistritbue isis** *tag1* **level-1 into level-2** cancels the redistribution of the routes of the IS-IS instance name *tag1*. **no redistritbue isis** *tag1* l**evel-1 into level-2 route-map** *aa* cancels the use of the route map named aa to filter redistributed routes.

Examples

The following example redistributes the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis aa
Hostname(config-router)# redistribute isis bb level-1 into level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis protocol**

1.70 redistribute isis level-2 into level-1

Function

Run the **redistribute isis level-2 into level-1** command to redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

Run the **no** form of this command to remove this configuration.

Redistribution is disabled by default.

Syntax

redistribute isis [*tag*] **level-2 into level-1** [**distribute-list** *acl-name* | { **prefix** *ipv4-address net-mask*| **ipv6-prefix** *ipv6-address/length*} | **route-map** *route-map-name*]

no redistribute isis [*tag*] **level-2 into level-1** [**distribute-list** *acl-name* | { **prefix** *ipv4-address net-mask*| **ipv6-prefix** *ipv6-address/length*} | **route-map** *route-map-name*]

Parameter Description

tag: Name of the IS-IS instance whose routing information will be redistributed.

distribute-list *acl-name*: Filters redistributed routes by using **distribute-list**. *access-list-name* indicates the associated prefix list, which can be a standard, an extended, or a name prefix list. The format is as follows:

{ *<1-99>* | *<100-199>* | *<1300-1999>* | *<2000-2699>* | *acl-name* }

In IS-IS IPv6 address family configuration mode, only the name prefix list can be used, in the format of *acl-name.*

prefix *ipv4-address net-mask*: Configures IPv4 routes that can be redistributed. Routes are specified by address and prefix length.

ipv6-prefix *ipv6-addressIlength*: Configures IPv6 routes that can be redistributed. Routes are specified by address and prefix length.

route-map *route-map-name*: Indicates the route map used for route redistribution. It is used to filter redistributed routes or configure the attributes of redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

You can use the **route-map**, **distribute-list**, or **prefix** parameter to filter the specified instance's Level-2 routes to be redistributed. Only the routes that meet specific criteria can be redistributed to Level-1 of the current instance.

The **route-map**, **distribute-list**, and **prefix** parameters cannot be used at the same time. If routes are filtered based on the prefix, only the Level-2 routes of local instance can be filtered.

The **no redistritbue isis** [**tag**] **level-2 into level-1** command is used to cancel the redistribution of the specified instance's routes. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution.

For example:

no redistritbue isis tag1 level-2 into level-1 cancels the redistribution of the routes of the IS-IS instance name tag1. **no redistritbue isis tag1 level-2 into level-1 route-map aa** cancels the use of the route map named aa to filter redistributed routes, rather than redistribution of the routes of the IS-IS instance name tag1.

Examples

The following example redistributes the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis aa
Hostname(config-router)# redistribute isis bb level-2 into level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis protocol**

1.71 router isis

Function

Run the **router isis** command to create an IS-IS instance.

Run the **no** form of this command to remove this configuration.

No IS-IS instance is configured by default.

Syntax

router isis [*tag*]

no router isis [*tag*]

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Use this command to initialize an IS-IS instance and enter IS-IS routing process configuration mode. An IS-IS instance will start running after a NET address is configured.

If you set the tag parameter when you start an IS-IS routing process, you need to add the tag parameter when closing the IS-IS routing process.

CPU protection is enabled by default. For packets sent to each destination group address (AllISSystems, AllL1ISSystems, and AllL2ISSystems), the number of packets sent to the CPU is limited to 400 per second. If a device has many neighbor relationships or sends Hello packets at short intervals, the IS-IS packets that the device receives may exceed the default limit, causing frequent flapping of neighbor relationships. To solve the problem, you can use the CPU protection command in global configuration mode to increase the limit.

Examples

The following example creates an IS-IS instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.72 set-overload-bit

Function

Run the **set-overload-bit** command to prevent neighbors from using the local IS-IS node as a forwarding device to forward data.

Run the **no** form of this command to remove this configuration.

A neighbor considers the local IS-IS node as a forwarding device to forward data by default.

Syntax

set-overload-bit [**on-startup** { *overload-time* | **wait-for-bgp** [*bgp-convergence-time*] }] [**suppress** { **external** | **interlevel** | **max-metric** } *] [**level-1** | **level-2**]

no set-overload-bit [**level-1** | **level-2**]

Parameter Description

on-startup: Indicates that an IS-IS node enters overload state temporarily after restart.

overload-time: Duration when an IS-IS node remains in overload state after restart, in seconds. The value range is from 5 to 86400, and the default value is **600**.

wait-for-bgp: Indicates that an IS-IS node automatically enters overload state after restart and waits for BGP convergence completion or timeout. This option is used with the keyword **on-startup**.

bgp-convergence-time: Time for waiting for BGP convergence completion, in seconds. The value range is from 5 to 86400, and the default value is **600**.

suppress: Indicates that an IS-IS node does not advertise internal routes (intra-area and inter-area routes) or external routes to neighbors when the IS-IS node is in overload state.

external: Indicates that an IS-IS node does not advertise external routes to neighbors when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

interlevel: Indicates that an IS-IS node does not advertise intra-area and inter-area routes to neighbors when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

max-metric: Sets the metric values of the advertised direct routes and neighbor reachable routes to the maximum values when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

level-1: Sends LSPs with the overload bit only to Level-1 neighbors.

level-2: Sends LSPs with the overload bit only to Level-2 neighbors.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

This command forces an IS-IS node to configure the overload bit in non-virtual LSPs to instruct its IS-IS neighbors to avoid using the local node as a forwarding device.

If the **on-startup** keyword is included, the IS-IS node temporarily enters overload state after restart. The overload bit is automatically configured or removed by the IS-IS node based on configuration.

If the **on-startup** keyword is not included, the IS-IS node enters overload state immediately after restart. The overload bit is configured or removed manually.

Note

At the same Level, the configuration with the **on-startup** keyword and the configuration without the **on-startup** keyword are mutually exclusive.

The overload bit is used in the following three situations:

- Device overload

The local IS-IS node has overload issues, such as insufficient memory or full CPU load; as a result, its routing table has incomplete routes or does not have resource forwarding data. You can configure the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

To configure the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually. When the local IS-IS node is restored, manually remove the command configuration; otherwise, the node is always in overload state.

- Instantaneous black hole

In the scenario described by RFC 3277, the IS-IS convergence speed is faster than the BGP speed; as a result, after an IS-IS node is restarted, a route may be instantaneously unreachable, which is called an instantaneous black hole. You can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device until the specified time has elapsed.

To set the overload bit, run the **set-overload-bit** command with the **on-startup** keyword. The overload bit can be configured or removed automatically by the IS-IS node based on the configuration.

After the **on-startup** keyword is selected, the IS-IS node automatically enters instantaneous black hole state after restart. When a neighbor relationship is established, the IS-IS node sends an LSP with the overload bit to notify the neighbor that the local node enters instantaneous black hole (or overload) state and instruct the neighbor to avoid using the local node as a forwarding device.

After the specified time has elapsed, the IS-IS node immediately sends an LSP with the overload bit canceled to notify the neighbor that the local node has exited instantaneous black hole (or overload) state and can work as a forwarding device.

The timer is configured based on the number of routes in the network. If there are a great number of routes in the network, the timer is set to a larger value. Otherwise, the timer is set to a smaller value.

- Disabling real data forwarding on the local IS-IS node

If you only need to connect the local IS-IS node to a production network for testing or to meet other functional requirements, but does not require the node to forward real data in the network, you can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

To set the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually.

You can set the **suppress** keyword based on requirements to limit the routing information carried in an LSP in case of overload. For example, internal and external routes can be suppressed, and only the local direct route is advertised. For example, the advertised direct route and the metric value to reach a neighbor are set to the maximum values.

Examples

The following example enables an IS-IS node to automatically enter overload state after restart and not to advertise internal routes (intra-area and inter-area routes) or external routes to neighbors in the wait time 300s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit on-startup 300 suppress interlevel external
```

The following example enables an IS-IS node not to advertise internal routes (intra-area and inter-area routes) or external routes to neighbors when the IS-IS node is in overload state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit suppress interlevel external
```

The following example enables an IS-IS node to automatically enter overload state after restart, wait for 300s, BGP route convergence completion or specified timer timeout, and set the metric values of the advertised direct routes and neighbor reachable routes to the maximum values.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit on-startup wait-for-bgp 300 suppress
max-metric
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis database**

1.73 show clns is-neighbors

Function

Run the **show clns is-neighbors** command to display all IS-IS neighbors and provide device adjacency relationship information.

Syntax

show clns [*tag*] **is-neighbors** [*interface-type interface-number*] [**detail**]

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Name of a specified interface.

detail: Displays detailed information of all interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all IS-IS neighbors and provides device adjacency relationship information.

```
Hostname> enable
Hostname# show clns is-neighbors detail
Area (null):
System Id   Type   IP Address   State  Holdtime  Circuit  Interface
r1         L1     1.0.0.2      Up     9       r1.01   TenGigabitEthernet 0/1
L2     1.0.0.2      Up     9       r1.01   TenGigabitEthernet 0/1
  Adjacency ID: 1
  Uptime: 00:00:54
  Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
  Level-2 MTID: Standard
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

Table 1-1 Output Fields of the show clns is-neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID
Type	Neighbor type
IP Address	IP address of the neighbor
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Circuit	Link ID
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
SNPA	SNPA address of the neighbor
IPv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology mode of the Level-1 neighbor
Level-2 MTID	Topology mode of the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.74 show clns neighbors

Function

Run the **show clns neighbors** command to display all IS-IS neighbors and provide device information and adjacency relationship information about terminals.

Syntax

show clns [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Name of a specified interface.

detail: Displays detailed information of all interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all IS neighbors and provides device information and adjacency relationship information about terminals.

```
Hostname> enable
Hostname# show clns neighbors detail
Area (null):
System Id     SNPA             State  Holdtime  Type Protocol Interface
r1           00d0.f8bc.de08     Up    7        L1   IS-IS    TenGigabitEthernet 0/1
                               Up    9        L2   IS-IS    TenGigabitEthernet 0/1
  Adjacency ID: 1
  Uptime: 00:01:40
  Area Address(es): 49.1111
IP Address(es): 1.0.0.2
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

Table 1-2 Output Fields of the show clns neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID
SNPA	SNPA address of the neighbor

Field	Description
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Type	Neighbor type
Protocol	Protocol type
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
IP Address(es)	IP Address
IPv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology mode of the Level-1 neighbor
Level-2 MTID	Topology mode of the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.75 show isis counter

Function

Run the **show isis counter** command to display statistical information of IS-IS.

Syntax

show isis [*tag*] **counter**

Parameter Description

Tag: Name of an IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example display statistical information of IS-IS.

```
Hostname> enable
Hostname# show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
isisSysStatLSPErrors: 0
IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
isisSysStatLSPErrors: 0
```

Table 1-3 Output Fields of the show isis counter Command

Field	Description
Area	Instance tag
IS-IS Level-1 isisSystemCounterEntry	Statistical table of the Level-1 system
isisSysStatCorrLSPs	Number of LSPs with length error
isisSysStatAuthTypeFails	Number of authentication failures with type error
isisSysStatAuthFails	Number of authentication failures with password inconsistency
isisSysStatLSPDbaseOloads	Number of overload times of the LSP database
isisSysStatManAddrDropFromAreas	Number of invalid area address drop times
isisSysStatAttmptToExMaxSeqNums	Number of LSP SNs exceeding maximum values
isisSysStatSeqNumSkips	Number of LSP SN skip times
isisSysStatOwnLSPPurges	Number of local failed LSPs
isisSysStatIDFieldLenMismatches	Number of system ID length mismatches
isisSysStatMaxAreaAddrMismatches	Number of maximum area address mismatches
isisSysStatPartChanges	Number of partition change times
isisSysStatSPFRuns	Number of SPF computation times
isisSysStatLSPErrors	Number of incorrect LSPs

Notifications

N/A

Platform Description

N/A

1.76 show isis database

Function

Run the **show isis database** command to display the information of an LSP database.

Syntax

show isis [*tag*] **database** [**detail** | **verbose**] [**l1** | **l2** | **level-1** | **level-2**] [*LSPID*]

Parameter Description

tag: Name of a specified IS-IS instance.

detail: Displays detailed information.

verbose: Displays more detailed information than **detail**.

l1 | **l2** | **level-1** | **level-2**: **l1** and **level-1**: Specify the Level-1 LSP database. **l2** and **level-2**: Specify the Level-2 LSP database.

LSPID: ID of the specified LSP. Only the corresponding LSP information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information of an LSP database.

```
Hostname> enable
Hostname# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime    ATT/P/OL
Hostname.00-00  * 0x00000007  0xCDD5       1011             0/0/0
  Area Address: 49.1111
  NLPID:       0xCC
  Hostname:    Hostname
  IP Address:   1.0.0.1
  Metric:   10       IS r1.01
  Metric:   10       IP 1.0.0.0 255.255.255.0
r1.00-00        0x00000006   0xA771       1032            0/0/0
  Area Address: 49.1111
  NLPID:       0xCC
  Hostname:    r1
  IP Address:   1.0.0.2
  Metric:   10       IS r1.01
  Metric:   10       IP 1.0.0.0 255.255.255.0
r1.01-00        0x00000002   0x062A       989             0/0/0
  Metric:   0        IS r1.00
  Metric:   0        IS Hostname.00
IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime    ATT/P/OL
Hostname.00-00  * 0x0000000A  0xC7D8        1033            0/0/0
  Area Address: 49.1111
  NLPID:       0xCC
  Hostname:    Hostname
  IP Address:   1.0.0.1
  Metric:   10       IS r1.01
```

```
  Metric:   10        IP 1.0.0.0 255.255.255.0
r1.00-00        0x00000006  0xA771        1032             0/0/0
  Area Address: 49.1111
  NLPID:       0xCC
  Hostname:     r1
  IP Address:   1.0.0.2
  Metric:   10        IS r1.01
  Metric:   10        IP 1.0.0.0 255.255.255.0
r1.01-00        0x00000002  0x062A        989              0/0/0
  Metric:   0         IS r1.00
Metric:   0         IS Hostname.00
```

Table 1-4 Output Fields of the show isis database detail Command

Field	Description
Area	Instance tag
IS-IS Level-1 Link State Database	Level-1 LSDB
LSPID	LSP ID
LSP Seq Num	LSP SN
LSP Checksum	LSP checksum
LSP Holdtime	LSP holdtime
ATT	Additional bit
P	Split bit
OL	Overload bit
Area Address	Area address
NLPID	Protocol supported by ISIS. **0xCC** indicates the IP protocol.
Hostname	Host name
IP Address	IP address
Metric	Metric

The following example displays the STLV information of an LSP database.

```
Hostname> enable
Hostname# show isis database verbose
IS-IS Level-1 Link State Database
LSPID              LSP Seq Num   LSP Checksum  LSP Holdtime  TT/P/OL
1111.1111.1111.00-00   0x00000005    0xB56A        1000        0/0/0
  Area Addres: 49
  NLPID:      0xCC
```

```
  Hostname: r1
  Router ID: 1.1.1.1
  IP Address: 192.17.10.2
  Metric: 10    IP  192.17.10.0/24
1111.1111.1111.01-00  0x00000002    0xBDCA        1020         0/0/0
  Metric: 10    IS-Extended 1111.1111.1111.00
  Affinity: 0x00000000
  Interface IP address: 192.17.10.2
  Physical BW: 10000000 bits/sec
  Reservable BW: 1000000 bits/sec
  BW Unreserved[0]: 1000000 bits/sec, BW Unreserved[1]: 1000000 bits/sec
  BW Unreserved[2]: 1000000 bits/sec, BW Unreserved[3]: 1000000 bits/sec
  BW Unreserved[4]: 1000000 bits/sec, BW Unreserved[5]: 1000000 bits/sec
  BW Unreserved[6]: 1000000 bits/sec, BW Unreserved[7]: 1000000 bits/sec
```

Table 1-5 Output Fields of the show isis database verbose Command

Field	Description
LSPID	LSP ID
LSP Seq Num	LSP SN
LSP Checksum	LSP checksum
LSP Holdtime	LSP holdtime
ATT	Additional bit
P	Split bit
OL	Overload bit
Area Address	Area address that this device can reach
NLPID	Network protocol ID
Hostname	Host name of the node
Router ID	TE router ID of the node
IP Address	IPv4 address of the interface
Metric	IS-IS metric
Affinity	Management group attribute described in the link
Physical BW	Actual bandwidth of the link
Reservable BW	Reserved bandwidth of the link
BW Unreserved	Reserved bandwidth for current priority

Notifications

N/A

Platform Description

N/A

1.77 show isis graceful-restart

Function

Run the **show isis graceful-restart** command to display the state information about IS-IS GR.

Syntax

show isis [*tag*] **graceful-restart**

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the state information about IS-IS GR.

```
Hostname> enable
Hostname# show isis graceful-restart
Area (null):
  Graceful-restart Helper: enabled
    Level 1:
      TenGigabitEthernet 0/1: RR received: 0
     Level 2:
      TenGigabitEthernet 0/1: RR received: 0
  Graceful-restart: enabled
    Graceful-period: 400s, Level timer: 60s, Interface timer: 3s
    Instance GR status: not restarting
```

Table 1-6 Output Fields of the show isis graceful-restart Command

Field	Description
Graceful-restart	Configuration state of the GR Restarter
Graceful-period	GR timer time
Level timer	Level-based timer time
Interface timer	Interface-based timer time
Graceful-restart Helper	Configuration state of the GR Helper
RR received	Statistics on received hello packets with the RR field
Instance GR status	GR state of the IS-IS instance

Notifications

N/A

Platform Description

N/A

1.78 show isis hostname

Function

Run the **show isis hostname** command to display the mapping of a host name to a system ID.

Syntax

show isis [*tag*] **hostname**

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mapping of a host name to a system ID.

```
Hostname> enable
Hostname# show isis hostname
```

```
  System ID     Dynamic Hostname     Area (null)
* 5555.5555.5555 Hostname
  1111.1111.1111 R1
  System ID     Dynamic Hostname     Area 1
* 4444.4444.4444 Hostname
  2222.2222.2222 R2
```

Table 1-7 Output Fields of the show isis hostname Command

Field	Description
System ID	System ID ● If the system ID is marked with an asterisk (*), the mapping of the local host name to a system ID is learned. ● If the system ID is not marked with an asterisk (*), the mapping of a non-local host name to a system ID is learned.
Dynamic Hostname	Host name
Area	Instance tag

Notifications

N/A

Platform Description

N/A

1.79 show isis interface

Function

Run the **show isis interface** command to display details of an IS-IS interface.

Syntax

show isis [*tag*] **interface** [*interface-type interface-number*] [**counter**]

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Interface type and interface number.

counter: Specifies the number of packet sending and receiving trigger times.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the details of an IS-IS interface.

```
Hostname> enable
Hostname# show isis interface
Area (null):
TenGigabitEthernet 0/1 is up, line protocol is up
  Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000001
    Local SNPA: 00d0.f822.33ab
    IP interface address:
      1.0.0.1/24
    Level-1 MTID: Standard
Level-2 MTID: Standard
Level-1 Metric: 10/10, Priority: 64, Circuit ID: r1.01
Level-1 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-1 LSPs in queue: 0
Level-1 LSPs flood: 5
    Number of active level-1 adjacencies: 1
Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01
Level-2 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-2 LSPs in queue: 0
Level-2 LSPs flood: 5
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 5 seconds
Next IS-IS LAN Level-2 Hello in 5 seconds
IS-IS TE: Enable
BFD Enabled (Anti-congestion)
```

Table 1-8 Output Fields of the show isis interface Command

Field	Description
Area	Instance tag
Routing Protocol	Routing protocol running on the interface

Field	Description
Network Type	Network type
Circuit Type	Link type
Local circuit ID	Local link ID
Extended Local circuit ID	ID of extended local link
Local SNPA	Local SNPA address
IP interface address	IP address of the interface
Level-1 MTID	Topology mode of the interface at Level-1
Level-2 MTID	Topology mode of the interface at Level-2
Level-1 Metric	Level-1 metric
Priority	Priority
Circuit ID	Link ID
Hello	Hello timer configuration on the interface
Lsp	LSP timer configuration on the interface
Psnp	PSNP timer configuration on the interface
Csnp	CSNP timer configuration on the interface
Retransmit	LSP retransmission timer configuration on the interface
Level-1 LSPs in queue	Number of LSPs in Level-1 queue
Level-1 LSPs flood	Number of LSPs sent at a time at Level-1
Number of active level-1 adjacencies	Number of Level-1 neighbors
Level-2 Metric	Level-2 metric
Level-2 LSPs in queue	Number of LSPs in Level-2 queue
Level-2 LSPs flood	Number of LSPs sent at a time at Level-2
Number of active level-2 adjacencies	Number of Level-2 neighbors
Next IS-IS LAN Level-1 Hello in 5 seconds	Next Level-1 hello packet sending time
Next IS-IS LAN Level-2 Hello in 5 seconds	Next Level-2 hello packet sending time

Field	Description
BFD Enabled(Anti-congestion)	BFD session state. If **Anti-congestion** is included, the BFD anti-congestion function is enabled. Otherwise, the anti-congestion function is not enabled.

The following example displays the statistical information of an IS-IS interface.

```
Hostname> enable
Hostname# show isis interface counter
Area (null):
TenGigabitEthernet 0/1:
   IS-IS LAN Level-1 isisCircuitCounterEntry:
     isisCircAdjChanges: 4
     isisCircNumAdj: 2
     isisCircInitFails: 0
     isisCircRejAdjs: 0
     isisCircIDFieldLenMismatches: 0
     isisCircMaxAreaAddrMismatches: 0
     isisCircAuthTypeFails: 0
     isisCircAuthFails: 0
     isisCircLanDesISChanges: 1
   IS-IS LAN Level-2 isisCircuitCounterEntry:
     isisCircAdjChanges: 4
     isisCircNumAdj: 2
     isisCircInitFails: 0
     isisCircRejAdjs: 0
     isisCircIDFieldLenMismatches: 0
     isisCircMaxAreaAddrMismatches: 0
     isisCircAuthTypeFails: 0
     isisCircAuthFails: 0
     isisCircLanDesISChanges: 1
   IS-IS Level-1 isisPacketCounterEntry:
     isisPacketCountIIHello in/out: 187/278
     isisPacketCountLSP in/out: 10/7
     isisPacketCountCSNP in/out: 0/92
     isisPacketCountPSNP in/out: 0/0
     isisPacketCountUnknown in/out: 0/0
   IS-IS Level-2 isisPacketCounterEntry:
     isisPacketCountIIHello in/out: 186/286
     isisPacketCountLSP in/out: 17/9
     isisPacketCountCSNP in/out: 1/91
     isisPacketCountPSNP in/out: 0/0
     isisPacketCountUnknown in/out: 0/0
```

Table 1-9 Output Fields of the show isis interface counter Command

Field	Description
IS-IS LAN Level-1 isisCircuitCounterEntry	Statistics of local Level-1 link
isisCircAdjChanges	Number of adjacency state change times on the local link
isisCircNumAdj	Number of adjacency times on the local link
isisCircInitFails	Number of initialization failure times on the local link
isisCircRejAdjs	Number of adjacency rejection times on the local link
isisCircIDFieldLenMismatches	Number of mismatches between the system ID in the received PDU and that in local system on the local link
isisCircMaxAreaAddrMismatches	Number of mismatches between the maximum number of area addresses in the received PDU and that in local system on the local link
isisCircAuthTypeFails	Number of mismatches between the authentication type in the received PDU and that in local system on the local link
isisCircAuthFails	Number of authentication failures due to mismatch of authentication passwords in the received PDU on the local link (authentication types match)
isisCircLanDesISChanges	Number of DIS changes at this level on the broadcast link
IS-IS LAN Level-2 isisCircuitCounterEntry	Statistics of the local Level-2 link
IS-IS Level-1 isisPacketCounterEntry	Packet statistics of the local Level-1 link
isisPacketCountIIHello in/out	Statistics about hello packet sending and receiving on the local link
isisPacketCountLSP in/out	Statistics about LSP packet sending and receiving on the local link
isisPacketCountCSNP in/out	Statistics about CSNP packet sending and receiving on the local link
isisPacketCountPSNP in/out	Statistics about PSNP packet sending and receiving on the local link
isisPacketCountUnknown in/out	Statistics about unknown packet sending and receiving on the local link
IS-IS Level-2 isisPacketCounterEntry	Packet statistics of the local Level-2 link

Notifications

N/A

Platform Description

N/A

1.80 show isis ipv6 topology

Function

Run the **show isis ipv6 topology** command to display the IPv6 unicast topology information of an IS-IS device.

Syntax

show isis [*tag*] **ipv6 topology** [**l1** | **l2** | **level-1** | **level-2**]

Parameter Description

tag: Name of a specified IS-IS instance.

l1: Specifies Level-1 topology.

level-1: Specifies Level-1 topology.

l2: Specifies Level-2 topology.

level-2: Specifies Level-2 topology.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the IPv6 unicast topology information.

```
Hostname> enable
Hostname# show isis ipv6 topology
Area (null):
IS-IS paths to level-1 routers
System Id   Metric   Next-Hop   SNPA            Interface
r1         10      r1       00d0.f822.33ad    TenGigabitEthernet 0/1
Hostname      -N/A
IS-IS paths to level-2 routers
System Id   Metric   Next-Hop   SNPA            Interface
r1         10      r1       00d0.f822.33ad    TenGigabitEthernet 0/1
Hostname      -N/A
```

Table 1-10 Output Fields of the show isis ipv6 topology Command

Field	Description
Area	Instance tag
System Id	System ID
Metric	Metric
Next-Hop	Next hop
SNPA	SNPA address
Interface	Interface name

Notifications

N/A

Platform Description

N/A

1.81 show isis mesh-groups

Function

Run the **show isis mesh-groups** command to display the mesh group configuration of interfaces.

Syntax

show isis [*tag*] **mesh-groups**

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mesh group configuration of all interfaces.

```
Hostname> enable
Hostname# show isis mesh-groups
Mesh group (blocked)
```

```
TenGigabitEthernet 0/1
Mesh group 1 :
TenGigabitEthernet 0/2
```

Table 1-11 Output Fields of the show isis mesh-groups Command

Field	Description
Mesh group (blocked) TenGigabitEthernet 0/1	Interface that blocks the mesh group
Mesh group 1 TenGigabitEthernet 0/2	Interface for mesh group 1

Notifications

-

Platform Description

N/A

1.82 show isis neighbors

Function

Run the **show isis neighbors** command to display neighbor information of IS-IS.

Syntax

show isis [*tag*] **neighbors** [**detail**]

Parameter Description

tag: Name of a specified IS-IS instance.

detail: Displays detailed information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays detailed neighbor information of IS-IS.

```
Hostname> enable
Hostname# show isis neighbors detail
Area (null):
System Id  Type  IP Address    State   Holdtime  Circuit  Interface
```

```
r1        L1    1.0.0.2      Up     9        r1.01    TenGigabitEthernet 0/1
L2    1.0.0.2      Up     9        r1.01    TenGigabitEthernet 0/1
  Adjacency ID: 1
  Uptime: 00:06:25
  Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

Table 1-12 Output Fields of the show isis neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID
Type	Neighbor type
IP Address	IP address of the neighbor
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Circuit	Link ID. When the network type is Broadcast, the circuit column describes the DIS considered by the neighbor r1.
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
SNPA	SNPA address of the neighbor
Ipv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology type supported by the Level-1 neighbor
Level-2 MTID	Topology type supported by the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor

Field	Description
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.83 show isis nsr

Function

Run the **show isis nsr** command to display NSR information of IS-IS.

Syntax

show isis [*tag*] **nsr**

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the NSR information of IS-IS.

```
Hostname> enable
Hostname# show isis nsr
NSR role: master
Area (null):
NSR: enable
NSR state: realtime
Area 1:
NSR: disable
```

Table 1-13 Output Fields of the show isis nsr Command

Field	Description
NSR role	NSR role
Area	Instance tag
NSR	Whether the instance is configured with the NSR
NSR state	NSR running state of an instance. It is displayed after the instance is configured with the NSR.

Notifications

N/A

Platform Description

N/A

1.84 show isis protocol

Function

Run the **show isis protocol** command to display protocol information of IS-IS.

Syntax

show isis [*tag*] **protocol**

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the protocol information of IS-IS.

```
Hostname> enable
Hostname# show isis protocol
IS-IS Router: (null)
  Binding VRF: vrf
  Mib-Binding: off
System ID: 0000.0000.0036   IS-type: level-2
Virtual System ID:
```

```
  1111.1111.1111, 2222.2222.2222
  Manual area address(es):
    49.0001, 49.0003
  Interfaces supported by IS-IS:
    TenGigabitEthernet 0/1, TenGigabitEthernet 0/2
  Redistributing IPv4:
isis 1, isis 2
Redistributing IPv6:
  isis 3, isis 4
  Distance: 115
  Generate narrow metrics:  Level-2
  Accept narrow metrics:    Level-2
  Generate wide metrics:    none
Accept wide metrics:     none
NSR: enable
Two-way-maintain: enable
BGP-LS: Level-2
```

Table 1-14 Output Fields of the show isis protocol Command

Field	Description
IS-IS Router	Instance tag
Binding VRF	VRF name bound to the IS-IS instance
Mib-Binding	Whether the instance is bound to SNMP operations
System ID	System ID
IS-type	Level type supported by the instance
Virtual System ID	Extended system ID
Manual area address(es)	Area ID
Interfaces supported by IS-IS	Interface associated with this instance
Redistributing IPv4	Source of the IPv4 redistributed route
Redistributing IPv6	Source of the IPv6 redistributed route
Distance	IS-IS management weight
Generate narrow metrics	Type of narrow metric generated
Accept narrow metrics	Type of narrow metric received
Generate wide metrics	Type of wide metric generated
Accept wide metrics	Type of wide metric received

Field	Description
NSR	Whether the instance is configured with the NSR. It is displayed when the instance is configured with the NSR.
Two-way-maintain	Whether the instance is configured with the two-way-maintain function
BGP-LS	Level type of the BGP-LS configured for the instance

Notifications

N/A

Platform Description

N/A

1.85 show isis topology

Function

Run the **show isis topology** command to display the topology information of connected IS-IS devices.

Syntax

show isis [*tag*] **topology** [**l1** | **l2** | **level-1** | **level-2**]

Parameter Description

tag: Name of a specified IS-IS instance.

l1: Specifies Level-1 topology.

level-1: Specifies Level-1 topology.

l2: Specifies Level-2 topology.

level-2: Specifies Level-2 topology.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the topology information of connected IS-IS devices.

```
Hostname> enable
Hostname# show isis topology
Area (null):
```

```
IS-IS paths to level-1 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1          10       r1         00d0.f822.33ad    TenGigabitEthernet 0/1
Hostname
IS-IS paths to level-2 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1          10       r1         00d0.f822.33ad    TenGigabitEthernet 0/1
Hostname
```

Table 1-15 Output Fields of the show isis protocol Command

Field	Description
Area	Instance tag
System Id	System ID
Metric	Metric
Next-Hop	Next hop
SNPA	SNPA address
Interface	Interface of next hop

Notifications

N/A

Platform Description

N/A

1.86 show isis virtual-neighbors

Function

Run the **show isis virtual-neighbors** command to display virtual system neighbor information of IS-IS.

Syntax

show isis [*tag*] **virtual-neighbors**

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays virtual system neighbor information of IS-IS.

```
Hostname> enable
Hostname# show isis virtual-neighbors
Area (null):
Virtual System Id          Type        State
1111.1111.1111             L1          DOWN
                          L2          UP
2222.2222.2222             L1          DOWN
                          L2          UP
```

Table 1-16 Output Fields of the show isis virtual-neighbors Command

Field	Description
Area	Instance tag
Virtual System Id	Virtual system ID
Type	Neighbor type
State	State of the neighbor. The value **Up** indicates that LSP fragments are created at the corresponding level.

Notifications

N/A

Platform Description

N/A

1.87 spf-interval

Function

Run the **spf-interval** command to configure the exponential backoff algorithm of SPF calculation.

Run the **no** form of this command to restore the default configuration.

The default maximum calculation interval of two SPF calculations is **10** seconds, the delay of the first SPF calculation is **50** ms, and the maximum interval for the first and second SPF calculations is **200** ms. Exponential backoff algorithm uses level-1/Level-2. That is, it takes effect for Level-1 and Level-2 concurrently.

Syntax

spf-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

no spf-interval [**level-1** | **level-2**]

Parameter Description

level-1: Takes effect for Level-1 IS-IS.

level-2: Takes effect for Level-2 IS-IS.

maximum-interval: Maximum interval for performing two consecutive SPF calculations, in seconds. The value range is from 1 to 120.

initial-interval: Wait time for performing the SPF calculation for the first time, in milliseconds. The value range is from 0 to 60000.

hold-interval: Minimum interval for performing the SPF calculation for the first and second times, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

Increasing the maximum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger minimum interval also leads to slower responses to route changes.

The wait time for performing the SPF calculation for the first time is the *initial-interval*. If the network becomes unstable, the SPF calculation interval is less than the *maximum-interval*, and the interval for performing the SPF calculation for the second time becomes the *hold-interval*. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the *maximum-interval*. Subsequent SPF calculations are performed at the *maximum-interval*. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the *maximum-interval*, and the wait time for performing the SPF calculation is restored to the *initial-interval*.

Link changes have high requirements for convergence. The initial interval can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.

Examples

The following example configures an exponential backoff algorithm of SPF calculation, and sets the maximum interval of two SPF calculations to **5** seconds, the wait time of SPF calculation for the first time to **100** ms, and the interval for the first and SPF calculation to **200** ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# spf-interval 5 100 200
```

The following example configures an exponential backoff algorithm of SPF calculation, sets the maximum interval of two SPF calculations to **10** seconds, and uses the default values of other exponential backoff parameters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# spf-interval 10
```

Notifications

If the configured value of *hold-interval* is greater than *maximum-interval* (for example, the configured value of *hold-interval* is **1500** ms, and the *maximum-interval* is **1** second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than maximum_interval (1s), set to
(1000ms).
```

If the configured value of *initial-interval* is greater than *hold-interval* (for example, the configured value of *initial-interval* is **20** ms, and the *hold-interval* is **10** ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set to
(10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.88 summary-address

Function

Run the **summary-address** command to configure IPv4 summarized routes.

Run the **no** form of this command to remove this configuration.

The route summarization function is disabled by default.

Syntax

summary-address *ipv4-address net-mask* [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*]

no summary-address *ipv4-address net-mask*

Parameter Description

ipv4-address: IPv4 address of the summarized route.

net-mask: Network mask of the summarized route.

level-1: Takes effect for Level-1 summarized routes.

level-1-2: Takes effect for Level-1 and Level-2 summarized routes.

level-2: Takes effect for Level-2 summarized routes.

metric-value: Metric of the summarized route. The value range is from 1 to 4294967295, and the default value is **0**.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the configured summarized route contains routing information about a reachable address or network segment, the summarized route, instead of detailed routes, is advertised externally.

Examples

The following example sets the IPv4 summarized route to 10.10.0.0/24 on Level-2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# summary-address 10.10.0.0 255.255.255.0 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP routing basic)

1.89 summary-prefix

Function

Run the **summary-prefix** command to configure IPv6 summarized routes.

Run the **no** form of this command to remove this configuration.

The route summarization function is disabled by default.

Syntax

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-1-2** | **level-2**]

no summary-prefix *ipv6-prefix/prefix-length*

Parameter Description

ipv6-prefix/prefix-length: Network address of the summarized route and its IPv6 prefix length. It follows the X:X:X:X::X/<0-128> format.

level-1: Takes effect for Level-1 summarized routes.

level-1-2: Takes effect for Level-1 and Level-2 summarized routes.

level-2: Takes effect for Level-2 summarized routes. By default, the setting takes effect for Level-2.

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

If the configured summarized route contains routing information about a reachable address or network segment, the summarized route, instead of detailed routes, is advertised externally.

Examples

The following example sets the IPv6 summarized route to 1000::/96 on Level-2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# summary-prefix 1000::/96 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv**6 **route** (IP routing basic)

1.90 two-way-maintain

Function

Run the **two-way-maintain** command to enable the two-way maintenance function of IS-IS.

Run the **no** form of this command to disable this function.

The two-way maintenance function is enabled by default.

Syntax

two-way-maintain

no two-way-maintain

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

In a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a result, some packets are delayed or discarded. If the time required for processing hello packets exceeds the neighbor holdtime, the corresponding adjacency times out and is removed. If the two-way maintenance function is enabled, in addition to the hello packets, the LSP, CSNP, and PSNP packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist in the network. This prevents termination of the adjacency caused by delayed or discarded hello packets.

Examples

The following example enables the two-way maintenance function of IS-IS.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# no two-way-maintain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis protocol**

1.91 virtual-system

Function

Run the **virtual-system** command to configure an additional system ID for fragment extension.

Run the **no** form of this command to disable this function.

The fragment extension function is disabled by default.

Syntax

virtual-system *system-id*

no virtual-system *system-id*

Parameter Description

system-id: ID of an additional system, six bytes.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure the additional system ID of an IS-IS routing process, which is used by the extended LSP that is generated after the 256 fragments of the original LSP are used up. To enable fragment extension, run this command to configure an additional system ID and run the **lsp-fragments-extend** command to configure fragment extension.

Examples

The following example sets the Additional system ID to 0000.0000.0034 for fragment extension.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# virtual-system 0000.0000.0034
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.92 vrf

Function

Run the **vrf** command to bind an IS-IS instance to a VRF table.

Run the **no** form of this command to remove this configuration.

VRF binding of an IS-IS instance is disabled by default.

Syntax

vrf *vrf-name*

no vrf *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Before you bind an IS-IS instance to a VRF table, ensure that the VRF table has been configured. If you need to establish an IS-IS IPv6 neighbor relationship, enable IPv6 and ensure that the table to be bound is a multiprotocol VRF table.

Note the following constraints or conventions for the binding operation:

- The IS-IS instances bound with the same non-default VRF table must be configured with different system IDs.
- The IS-IS instances bound with different VRF tables can be configured with the same system ID.
- One IS-IS instance can be bound with only one VRF table, but one VRF table can be bound to multiple IS-IS instances.
- When the VRF table bound to an IS-IS instance is changed, all IS-IS interfaces associated with the instance will be deleted. That is, the **ip** (or **ipv6**) **router isis [tag]** interface configuration and the redistribution configuration in routing process configuration mode will be deleted.

Examples

The following example binds an IS-IS instance to vrf_1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf_1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# exit-address-family
Hostname(config)# router isis
Hostname(config-router)# vrf vrf_1
```

Notifications

If the VRF bound does not exist, the following notification will be displayed:

```
% The VRF does not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show isis protocol**

1 BGP Commands

Command	Function
address port	Configure the address and port number of a BGP Monitoring Protocol (BMP) server.
address-family ipv4	Enter the IPv4 address family mode of Border Gateway Protocol (BGP).
address-family ipv4 vrf	Enter the IPv4 VRF address family mode of BGP and enable the exchange function of VRF routing information.
address-family ipv6	Enter the IPv6 address family mode of BGP and enable the exchange function of IPv6 routing information of BGP.
address-family ipv6 vrf	Enter the IPv6 VRF address family mode and enable the exchange function of IPv6 routing information of a VRF instance.
adj-rib-in post-policy	Configure BMP to monitor the routing information received from a peer after the routing policy is applied.
adj-rib-in pre-policy	Configure BMP to monitor the unchanged routing information received from a peer.
adj-rib-out post-policy	Configure BMP to monitor the routes sent to a peer after the routing policy is applied.
aggregate-address	Configure a route aggregation entry of BGP.
bgp additional-paths select	Enable the selection function of alternative additional paths (ADD-PATH) routes.
bgp advertise lowest-priority on-startup	Adjust the priority of routes advertised during device restart to the lowest level.
bgp advertise non-transitive extcommunity	Add the non-transmissive extended community attribute when BGP advertises routes to an External BGP (EBGP) neighbor.
bgp advertise-map	Match a global routing policy with sent routes.
bgp always-compare-med	Enable the Multi Exit Discriminator (MED) comparison function of BGP.

bgp asnotation dot	Display 4-byte AS numbers in dot mode and match regular expressions. Two decimals are separated by dot, for example 65535.65535.
bgp bestpath aigp ignore	Disable AIGP metric value comparison when the optimal path is selected.
bgp bestpath as-path ignore	Not compare AS path length when the optimal path is selected.
bgp bestpath as-path multipath-relax	Enable AS-PATH loose comparison of multiple paths in load balancing mode for BGP.
bgp bestpath compare-confed-aspath	Compare AS path length when the optimal path is selected.
bgp bestpath compare-routerid	Compare path router IDs when the optimal path is selected.
bgp bestpath igp-metric ignore	Not compare the next-hop IGP metric values when the optimal path is selected.
bgp bestpath med confed	Compare path MED values from the same AS alliance when the optimal path is selected.
bgp bestpath med missing-as-worst	Set the priority of a path without the MED attribute to the lowest level when the optimal path is selected.
bgp bestpath multipath-compare-routerid	Enable the function of comparing router IDs of multiple paths in load balancing mode.
bgp bmp-active	Enable all BMP servers to monitor all BGP neighbors.
bgp client-to-client reflection	Enable the route reflection function between device clients.
bgp cluster-id	Configure the cluster ID for a route reflector.
bgp confederation identifier	Configure an ID for an AS alliance.
bgp confederation peers	Configure a member AS for an AS alliance.
bgp dampening	Enable the route dampening function and configure dampening parameters.
bgp default ipv4-unicast	Configure the default address family as the IPv4 unicast address family.
bgp default local-preference	Configure the default LOCAL_PREF attribute.
bgp default route-target filter	Enable the Route-Target filtering function.

bgp deterministic-med	Preferentially compare path MED values for peers from the same AS.
bgp dmzlink-bw	Advertise bandwidth of a specified interface as an extended attribute.
bgp enforce-first-as	Configure a device to check the first AS number of the AS_PATH field in update packets.
bgp fast-external-fallover	Enable the fast link detection function of EBGP neighbors.
bgp fast-reroute	Enable the fast rerouting (FRR) function of BGP.
bgp fast-withdraw	Enable the fast withdrawal function of a specified BGP route.
bgp graceful-restart	Enable the function of global BGP graceful restart (GR).
bgp graceful-restart disable	Disable the GR function of a specified BGP address family.
bgp graceful-restart restart-time	Configure the GR time of BGP.
bgp graceful-restart stalepath-time	Configure the hold time of a stale route by a GR Helper during BGP GR.
bgp initial-advertise-delay	Enable the function of BGP delayed advertisement upon system restart.
bgp install standby-path	Enable the function of standby path installation of BGP.
bgp link-state-group up-delay	Configure the delay time to unbind the downlink port in the link state tracking group associated with the BGP neighbors.
bgp log-neighbor-changes	Configure a device to record BGP state changes without enabling the debugging function.
bgp maxas-limit	Limit the quantity of AS numbers in the AS_PATH attribute for BGP routes.
bgp maximum-neighbor	Configure the maximum number of BGP neighbors.
bgp maximum-prefix	Configure the maximum number of route entries in global configuration mode or for specified VRF instances.
bgp mp-error-handle session-retain	Configure BGP to retain BGP sessions when it detects a multiprotocol route error.

bgp nexthop trigger delay	Configure a delay of updating the routing table after the next hop of a BGP route changes.
bgp nexthop trigger enable	Enable the function of next hop trigger update.
bgp notify unsupport-capability	Enable the detection function of neighbor address family capability.
bgp nsr	Enable the global non-stop routing (NSR) function of BGP.
bgp recursion host	Enable BGP routes to recurse to only host routes.
bgp redistribute-internal	Configure BGP to allow the routes received from IBGP neighbors to be redistributed to Interior Gateway Protocol (IGP).
bgp route-reflector attribute-change	Allow the route reflector to modify route attributes.
bgp router-id	Configure a router ID when the BGP is running.
bgp scan-rib disable	Update the routing table in event triggering mode.
bgp scan-time	Configure the interval of regular scanning of BGP.
bgp shutdown	Actively shut down all connections.
bgp sourced-paths	Import routes with multiple paths or multiple next hops from other protocol modules.
bgp tcp-source-check disable	Disable the function of TCP source address checking of BGP.
bgp timer accuracy-control	Enable the strict execution function of internal timers of BGP.
bgp upgrade-cli	Configure the CLI display mode of BGP as address family configuration mode or scope configuration mode.
bmp server	Configure a BMP server instance and enter the BMP configuration mode.
buffer-size	Configure the maximum number of packets or bytes in the buffer of a BMP instance.
clear bgp advertise lowest-priority on-startup	Restore the priority of advertised routes to BGP neighbors to the level before the configuration of the **bgp advertise lowest-priority on-startup** command.
clear bgp all	Clear all the address families of BGP.

clear bgp all peer-group	Clear a specified peer group of BGP.
clear bgp all update-group	Clear the sessions of all members in an update group.
clear bgp ipv4 unicast	Clear the specified sessions of an IPv4 unicast address family.
clear bgp ipv4 unicast dampening	Clear the route flapping information of an IPv4 unicast address family and remove route dampening.
clear bgp ipv4 unicast external	Clear the EBGP connections of all IPv4 unicast address families.
clear bgp ipv4 unicast flap-statistics	Clear the statistics about route flapping of an IPv4 unicast address family.
clear bgp ipv4 unicast peer-group	Clear the sessions of all members of a peer group in an IPv4 unicast address family.
clear bgp ipv4 unicast table-map	Clear and update the Table-map configuration of an IPv4 unicast address family of BGP.
clear bgp ipv4 unicast update-group	Clear the sessions of all members of an update group in an IPv4 unicast address family.
clear bgp ipv6 unicast	Clear the specified sessions of an IPv6 unicast address family of BGP.
clear bgp ipv6 unicast dampening	Clear the route flapping information and route dampening of an IPv6 unicast address family.
clear bgp ipv6 unicast external	Clear all the EBGP connections of an IPv6 unicast address family.
clear bgp ipv6 unicast flap-statistics	Clear the statistics about route flapping of an IPv6 unicast address family.
clear bgp ipv6 unicast peer-group	Clear the sessions of all members of a peer group in an IPv6 unicast address family.
clear bgp ipv6 unicast table-map	Clear and update the Table-map configuration of an IPv6 unicast address family.
clear bgp ipv6 unicast update-group	Clear all the member sessions of an update group in an IPv6 unicast address family.
clear bmp	Reset BMP.
clear ip bgp	Clear the specified sessions of an IPv4 unicast address family of BGP.

clear ip bgp dampening	Clear the route flapping information and route dampening of an IPv4 unicast address family.
clear ip bgp external	Clear EBGP connections of all IPv4 unicast address families.
clear ip bgp flap-statistics	Clear statistics about route flapping of an IPv4 unicast address family.
clear ip bgp peer-group	Clear sessions of all members in a peer group in an IPv4 unicast address family.
clear ip bgp table-map	Clear old information and update the Table-map's routing information in an IPv4 unicast address family.
clear ip bgp update-group	Clear sessions of all members in a peer group in an IPv4 unicast address family.
default-information originate	Configure BGP to advertise redistributed default routes.
default-metric	Use the manually configured metric value for a redistributed route of BGP.
description	Configure description information of a BMP instance.
distance bgp	Configure the administrative distance of a BGP route.
exit-address-family	Exit the address family configuration mode of BGP.
failure-retry-delay	Configure the time to reestablish a connection with a BMP server.
import path selection	Configure a route import policy.
maximum-paths	Configure EBGP/IBGP multipath load balancing and specify the number of equivalent paths.
maximum-prefix	Configure the maximum number of route prefixes in a routing information base under an address family.
neighbor activate	Activate neighbors or peer groups in current address mode.
neighbor additional-paths	Enable the ADD-PATH function of the specified peer.
neighbor advertise additional-paths	Advertise the specific type of alternative ADD-PATH routes to peers.
neighbor advertisement-interval	Configure the route update interval of BGP.
neighbor aigp	Enable the AIGP function of BGP neighbors.

neighbor allowas-in	Allow the local device to receive update packets that carry the AS number of the local device.
neighbor as-loop-check out	Enable the loop detection function in the outbound direction of a BGP neighbor.
neighbor as-origination-interval	Configure the interval of advertising the local initial BGP route to a specified peer.
neighbor as-override	Configure a PE device to overwrite the AS number of a site.
neighbor bmp-active	Configure a specified BMP server to monitor neighbors.
neighbor default-fast-withdraw	Allow a BGP speaker to quickly withdraw the default route from a peer (group).
neighbor default-originate	Allow a BGP speaker to advertise the default route to a peer (group).
neighbor description	Configure the description statement of a specified peer (group).
neighbor distribute-list	Implement an ACL-based routing policy when routing information is sent to and received from a specified BGP peer.
neighbor dmzlink-bw	Carry the link bandwidth attribute in the specified neighbor's routes sent to IBGP neighbors.
neighbor domain	Configure a domain group for a specified BGP peer.
neighbor domain-unsuppress	Disable the domain group of a specified BGP peer from suppressing detailed routes.
neighbor ebgp-multihop	Establish BGP connections with non-directly-connected EBGP peers.
neighbor fall-over bfd	Correlate BGP with Bidirectional Forwarding Detection (BFD).
neighbor filter-list	Apply the AS path filtering rule to the routing information received from and sent to a specified BGP peer (group).
neighbor global-nexthop-replace-local	Use the local address of a BGP IPv6 link as the global next hop address when IPv6 routing information is sent to the local peer (group) of the BGP IPv6 link.

neighbor ha-mode nsr	Enable the nonstop routing (NSR) function for a specified BGP peer (group).
neighbor link state group	Associate a BGP peer (group) with a link state tracking group.
neighbor local-as	Configure the local AS number for a specified BGP peer (group).
neighbor maximum-prefix	Configure the maximum number of prefixes received from a specified BGP peer.
neighbor next-hop-self	Configure the next hop of a route advertised to a specified BGP peer as the local device.
neighbor next-hop-unchanged	Retain the next hop of a route advertised to a specified peer (group).
neighbor password	Enable TCP MD5 authentication and configure a password when a BGP connection is established with a specified BGP peer.
neighbor peer-group (assigning members)	Configure a specified BGP peer as a member of a BGP peer group.
neighbor peer-group (creating)	Create a BGP peer group.
neighbor pic-disable	Disable the private PIC processing on routes distributed to and received from specified BGP peers.
neighbor prefix-list	Implement the prefix list-based routing policy for routing information sent to and received from the specified BGP peers.
neighbor remote-as	Configure a BGP peer (group).
neighbor remove-private-as	Remove the private AS number from the AS_PATH attribute of the routes sent to a specified EBGP peer.
neighbor route-map	Match a received or an advertised route with a route map.
neighbor route-reflector-client	Configure the local device as a route reflector and specify a client for it.
neighbor send-community	Advertise community attributes to a specified BGP neighbor.
neighbor shutdown	Shut down the connection of a specified peer.

neighbor soft-reconfiguration inbound	Save original routing information sent by a specified BGP peer.
neighbor soo	Configure the Site-of-Origin (SoO) attribute of a neighbor.
neighbor timers	Configure the duration of Keepalive, Hold-Time, and Connect-Retry timers that are used to establish a BGP connection with a specified BGP peer.
neighbor transport connection-mode	Configure the connection establishment mode of BGP neighbors.
neighbor ttl-security hops	Configure GTSM security check for BGP neighbors.
neighbor unsuppress-map	Selectively advertise the routing information that is suppressed by route aggregation.
neighbor update-delay	Delay the advertisement of BGP peers.
neighbor update-source	Configure a network interface used to establish a BGP connection with a specified IBGP peer.
neighbor version	Configure the BGP version number for a specified BGP peer.
neighbor weight	Configure a weight value for a specified BGP peer.
network	Add static routing entries to a BGP routing table and advertise them to peers.
network synchronization	Synchronize a device with the local route to advertise the routing information configured by the network command.
overflow memory-lack	Configure BGP to enter the overflow state when the memory is insufficient.
redistribute	Redistribute the routing information of another routing protocol to a BGP instance.
redistribute isis	Redistribute the routing information of the IS-IS routing protocol to a BGP instance.
redistribute ospf	Redistribute the routing information of the Open Shortest Path First (OSPF) routing protocol to a BGP instance.
route mirroring	Enable the function of BGP packet mirroring.
router bgp	Enable the BGP protocol, configure a local AS number, and enter the BGP configuration mode.

scope	Enter the scope configuration mode and associate a VRF instance with BGP.
show bgp all	Display all the routing information of BGP.
show bgp bmp	Display BMP server information.
show bgp develop	Display the development information of BGP.
show bgp grst	Display GR information.
show bgp hash-peer	Display the hash table information of all neighbors.
show bgp ipv4 unicast	Display the IPv4 unicast routing information in BGP routing information.
show bgp ipv4 unicast dampening	Display the BGP IPv4 unicast route flapping information.
show bgp ipv4 unicast neighbors	Display the IPv4 unicast neighbor information of BGP.
show bgp ipv4 unicast paths	Display the IPv4 unicast path information in a routing information base.
show bgp ipv4 unicast summary	Display the BGP IPv4 unicast summary information.
show bgp ipv4 unicast update-group	Display the BGP IPv4 unicast update group information.
show bgp ipv6 unicast	Display the IPv6 unicast routing information in BGP routing information.
show bgp ipv6 unicast dampening	Display the IPv6 unicast route flapping parameters configured by BGP.
show bgp ipv6 unicast neighbors	Display the IPv6 unicast neighbor information of BGP.
show bgp ipv6 unicast paths	Display the IPv6 unicast path information in a routing information base.
show bgp ipv6 unicast summary	Display the BGP IPv6 unicast summary information.
show bgp ipv6 unicast update-group	Display the BGP IPv6 unicast update group information.
show bgp log-info	Display BGP log information.
show bgp log-warn	Display BGP alarm information.
show bgp memory	Display BGP memory information.
show bgp nsr	Display NSR information.

show bgp route-block	Display black hole route statistics.
show bgp rpi	Display RPI policy information.
show bgp statistics	Display BGP statistics.
show ip bgp	Display the routing information of an IPv4 unicast address family of BGP.
stats-reporting-period	Configure the interval of regularly sending state statistics by BGP.
synchronization	Enable the function of routing information synchronization between BGP and IGP.
table-map	Control the routing information sent to the core routing table by BGP.
timers bgp	Configure the duration of BGP timers.
update-source	Configure a network interface used to establish a TCP connection with a specified BMP server.

1.1 address port

Function

Run the **address port** command to configure the address and port number of a BGP Monitoring Protocol (BMP) server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BMP server is configured with address or port number by default.

Syntax

address { *bmp-server-ipv4-address* | *bmp-server-ipv6-address* } **port** *port-number*

no address { *bmp-server-ipv4-address* | *bmp-server-ipv6-address* } **port** *port-number*

default address { *bmp-server-ipv4-address* | *bmp-server-ipv6-address* } **port** *port-number*

Parameter Description

bmp-server-ipv4-address: IPv4 address of a specified BMP server.

bmp-server-ipv6-address: IPv6 address of a specified BMP server.

port-number: Listening port number of a specified BMP server.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the address of the specified BMP server to 10.0.0.1 and the port number to 12345.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# address 10.0.0.1 port 12345
```

Notifications

N/A

Common Errors

The address of the BMP server is a local address.

```
% Cannot configure the local system as bmp server
```

Platform Description

N/A

Related Commands

- **bmp server**

1.2 address-family ipv4

Function

Run the **address-family ipv4** command to enter the IPv4 address family mode of Border Gateway Protocol (BGP).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BGP is configured with the IPv4 unicast address family mode by default.

Syntax

address-family ipv4 [**unicast**]

no address-family ipv4 [**unicast**]

default address-family ipv4 [**unicast**]

Parameter Description

unicast: Enters the IPv4 unicast address family mode. If this parameter is not specified, BGP enters the IPv4 unicast address family mode.

Command Modes

BGP configuration mode

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can enter the configuration mode of the IPv4 address family of BGP to configure routes and neighbors of the IPv4 address family. Or, you can configure IPv4 neighbors in the BGP configuration mode, and activate them in the configuration mode of the IPv4 address family.

The **exit-address-family** command is configured to exit the configuration mode of the IPv4 address family.

Examples

The following example enters the IPv4 unicast address family mode of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv4 unicast
Hostname(config-router-af)#
```

Notifications

If configuration is completed in the scope Virtual Routing Forwarding (VRF) mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Invalid address family ipv4 unicast vrf vrf-name.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exit-address-family**

1.3 address-family ipv4 vrf

Function

Run the **address-family ipv4 vrf** command to enter the IPv4 VRF address family mode of BGP and enable the exchange function of VRF routing information.

Run the **no** form of this command to remove this configuration and disable this function.

Run the **default** form of this command to restore the default configuration.

No IPv4 VRF address family of BGP is configured by default.

Syntax

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

default address-family ipv4 vrf *vrf-name*

Parameter Description

vrf-name: VRF name.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

In the IPv4 VRF address family mode of BGP, you can configure Provider Edge (PE) or Multi-VPN-Instance Customer Edge (MEC) devices to exchange BGP routing information with Customer Edge (CE) devices.

The **exit-address-family** command is configured to exit the configuration mode of the IPv4 VRF address family.

Note

If the **scope** command is not configured to associate a VRF instance with BGP, the **neighbor** command configured in the **address-family ipv4 vrf** command is displayed in the **address-family ipv6 vrf** command.

Examples

The following example enables the exchange function of routing information for VRF VPN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv4 vrf vpn1
```

Notifications

If no VRF instance is configured, the following notification will be displayed:

```
% VRF vrf-name does not exist!
```

If the VRF instance is not configured with an RD, the following notification will be displayed:

```
% VRF vrf-name does not have an RD configured.
```

If the VRF instance does not activate the IPv4 address family, the following notification will be displayed:

```
% Invalid address family ipv4 unicast vrf %s.
```

If the BGP instance does not automatically obtain a router ID, the following notification will be displayed:

```
%Warning: The router identifier is 0.0.0.0, use 'bgp router-id' to configure a valid identifier.
```

If the command configuration fails due to other reasons, the following notification will be displayed:

```
% Can not bind vrf!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exit-address-family**

1.4 address-family ipv6

Function

Run the **address-family ipv6** command to enter the IPv6 address family mode of BGP and enable the exchange function of IPv6 routing information of BGP.

Run the **no** form this command to remove this configuration and disable this function.

Run the **default** form of this command to restore the default configuration.

No IPv6 address family of BGP is configured by default.

Syntax

address-family ipv6 [**unicast**]

no address-family ipv6 [**unicast**]

default address-family ipv6 [**unicast**]

Parameter Description

unicast: Enters the configuration mode of the IPv6 unicast address family. This parameter is optional. If this parameter is not specified, BGP enters the IPv6 unicast address family mode.

Command Modes

BGP configuration mode

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can enter the configuration mode of the IPv6 address family of BGP to configure routes and neighbors of the IPv6 address family. Or, you can configure IPv6 neighbors in the BGP configuration mode, and activate them in the configuration mode of the IPv6 address family.

The **exit-address-family** command is configured to exit the configuration mode of the IPv6 address family.

Examples

The following example enters the IPv6 address family mode of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv6
```

Notifications

If the global IPv6 unicast routing capability is not activated, the following notification will be displayed:

```
% IPv6 routing not enabled, BGP process can't configure
```

If configuration is completed in the scope VRF mode and the IPv6 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Invalid address family ipv6 unicast vrf vrf-name.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exit-address-family**

1.5 address-family ipv6 vrf

Function

Run the **address-family ipv6 vrf** command to enter the IPv6 VRF address family mode and enable the exchange function of IPv6 routing information of a VRF instance.

Run the **no** form of this command to remove this configuration and disable this function.

Run the **default** form of this command to restore the default configuration.

No IPv6 VRF address family is configured by default.

Syntax

address-family ipv6 vrf *vrf-name*

no address-family ipv6 vrf *vrf-name*

default address-family ipv6 vrf *vrf-name*

Parameter Description

vrf-name: VRF name.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

In the IPv6 VRF address family mode of BGP, you can configure PE or MEC devices to exchange BGP routing information with CE devices.

The **exit-address-family** command is configured to exit the configuration mode of the IPv6 VRF address family.

Note

If the **scope** command is not configured to associate a VRF instance with BGP, the **neighbor** configured in the **address-family ipv6 vrf** command in global configuration mode is displayed in the **address-family ipv4 vrf** command. Commands configured for single address families are displayed in the address family mode only configured by the commands.

Examples

The following example enables the IPv6 routing exchange capability for VRF VPN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv6 vrf vpn1
```

Notifications

If no VRF instance is configured, the following notification will be displayed:

```
% VRF vrf-name does not exist!
```

If the VRF instance is not configured with a Route Distinguisher (RD), the following notification will be displayed:

```
% VRF vrf-name does not have an RD configured.
```

If the VRF instance does not activate the IPv6 address family, the following notification will be displayed:

```
% Invalid address family ipv6 unicast vrf %s.
```

If the global IPv6 unicast routing capability is not activated, the following notification will be displayed:

```
% IPv6 routing not enabled,BGP IPv6 can't configure
```

If the BGP instance does not automatically obtain a router ID, the following notification will be displayed:

```
% Warning: The router identifier is 0.0.0.0, use 'bgp router-id' to configure a valid identifier.
```

If the command configuration fails due to other reasons, the following notification will be displayed:

```
% Can not bind vrf!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exit-address-family**

1.6 adj-rib-in post-policy

Function

Run the **adj-rib-in post-policy** command to configure BMP to monitor the routing information received from a peer after the routing policy is applied.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

BMP is not enabled to monitor the routing information received from a peer after the routing policy is applied.

Syntax

adj-rib-in post-policy

no adj-rib-in post-policy

default adj-rib-in post-policy

Parameter Description

N/A

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures BMP to monitor the routes received from a peer after the routing policy is applied.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# adj-rib-in post-policy
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 adj-rib-in pre-policy

Function

Run the **adj-rib-in pre-policy** command to configure BMP to monitor the unchanged routing information received from a peer.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

BMP is not configured to monitor the unchanged routing information received from a peer.

Syntax

adj-rib-in pre-policy

no adj-rib-in pre-policy

default adj-rib-in pre-policy

Parameter Description

N/A

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures BMP to monitor the unchanged routing information received from a peer.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# adj-rib-in pre-policy
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 adj-rib-out post-policy

Function

Run the **adj-rib-out post-policy** command to configure BMP to monitor the routes sent to a peer after the routing policy is applied.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

BMP is not configured to monitor the function of sending routes to a peer after the routing policy is applied.

Syntax

adj-rib-out post-policy

no adj-rib-out post-policy

default adj-rib-out post-policy

Parameter Description

N/A

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures BMP to monitor the routes sent to a peer after the routing policy is applied.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# adj-rib-out post-policy
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 aggregate-address

Function

Run the **aggregate-address** command to configure a route aggregation entry of BGP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No route aggregation entry of BGP is configured by default.

Syntax

aggregate-address { *ipv4-address mask* | *prefix* } [**advertise-map** route-map-name | **as-set** | **attribute-map** *route-map-name* | **summary-only** | **suppress-map** route-map-name] *

no aggregate-address { *ipv4-address mask* | *prefix* }

default aggregate-address { *ipv4-address mask* | *prefix* }

Parameter Description

ipv4-address: Aggregated IPv4 address.

mask: Mask of an aggregated IPv4 address.

prefix: Prefix of an aggregated IPv4 address.

advertise-map *route-map-name*: Configures a policy to generate route aggregation. *route-map-name* is the name of a route map and does not exceed 32 characters in length.

as-set: Reserves the AS path information within the aggregate address range. If this parameter is not specified, the AS path information within the aggregate address range is not reserved.

attribute-map *route-map-name*: Configures a route policy to control route aggregation attributes. *route-map-name* is the name of a route map and does not exceed 32 characters in length.

summary-only: Advertises only aggregate paths. If this parameter is not specified, all paths are advertised.

suppress-map *route-map-name*: Suppresses the route map of a specified route. *route-map-name* is the name of a route map and does not exceed 32 characters.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

All path information before and after aggregation is advertised by default. If only path information after aggregation needs to be advertised, specify the **summary-only** parameter during configuration.

Examples

The following example configures IPv4 route aggregation entries and reserves the AS path information within the aggregate path range.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Notifications

If the entered network address is invalid, the following notification will be displayed:

```
% Invalid network address
```

When the configured route aggregation entry is already configured, the following notification will be displayed:

```
% The same object already exists
```

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

If the deleted route aggregation entry is not configured, the following notification will be displayed:

```
% Unknown object, configure first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 bgp additional-paths select

Function

Run the **bgp additional-paths select** command to enable the selection function of alternative additional paths (ADD-PATH) routes.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The selection function of alternative ADD-PATH routes is disabled by default.

Syntax

bgp additional-paths select { **all** | **best** *best-number* | **ecmp** }

no bgp additional-paths select

default bgp additional-paths select

Parameter Description

all: Selects all valid routes as alternative ADD-PATH routes of the "all" type.

best *best-number*: Selects the next-best routes as alternative ADD-PATH routes of the "best number" type. The value of *best-number* is **2** or **3**.

ecmp: Selects the Equal-Cost Multipath Routing (ECMP) routes as alternative ADD-PATH routes of the "ECMP" type. You also need to select ECMP routes.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Default Level

14

Usage Guidelines

To advertise alternative ADD-PATH routes, you need to run the **neighbor advertise additional-paths** and **neighbor additional-paths** commands.

Examples

The following example selects the next-best routes as alternative ADD-PATH routes of the "best number" type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp additional-paths select best 2
```

The following example selects the alternative ADD-PATH routes of the "ECMP" type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# maximum-paths ibgp 8
Hostname(config-router)# bgp bestpath as-path multipath-relax
Hostname(config-router)# bgp additional-paths select ecmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **neighbor additional-paths**
- **bgp additional-paths select**
- neighbor advertise additional-paths

1.11 bgp advertise lowest-priority on-startup

Function

Run the **bgp advertise lowest-priority on-startup** command to adjust the priority of routes advertised during device restart to the lowest level.

Run the **no** form of this command to remove this configuration.

Run the **default** form of command to restore the default configuration.

BGP does not modify the priority of advertised routes by default.

Syntax

bgp advertise lowest-priority on-startup [*recover-time*]

no bgp advertise lowest-priority on-startup

default bgp advertise lowest-priority on-startup

Parameter Description

recover-time: Timer time in seconds at which the priority of advertised routes is restored. The value range is from 1 to 65535, and the default value is **600**.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

You can run this command to restore the priority of advertised routes to the original level before adjustment.

Examples

The following example configures BGP to adjust the priority of advertised routes to the lowest level upon device restart.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp advertise lowest-priority on-startup
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 bgp advertise non-transitive extcommunity

Function

Run the **bgp advertise non-transitive extcommunity** command to add the non-transmissive extended community attribute when BGP advertises routes to an External BGP (EBGP) neighbor.

Run the **no** form of this command to remove this configuration.

Run the **default** form of command to restore the default configuration.

BGP does not carry the non-transmissive extended community attribute when it advertises routes to an EBGP neighbor.

Syntax

bgp advertise non-transitive extcommunity

no bgp advertise non-transitive extcommunity

default bgp advertise non-transitive extcommunity

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

A device does not advertise the non-transmissive extended community attribute to a neighbor when it advertises routes to an EBGP peer. This command is configured to forcibly advertise the non-transmissive extended community attribute.

Routing information advertised to EBGP neighbors and Internal BGP (IBGP) neighbors of an alliance carries the non-transmissive extended community attribute.

Examples

The following example configures BGP to carry the non-transmissive extended community attribute when it advertises routes to an EBGP peer.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp advertise non-transitive extcommunity
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show bgp all**

1.13 bgp advertise-map

Function

Run the **bgp advertise-map** command to match a global routing policy with sent routes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No global routing policy matches routes sent to neighbors by default.

Syntax

bgp advertise-map *route-map-name*

no bgp advertise-map

default bgp advertise-map

Parameter Description

route-map-name: Name of a matched route map.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv4 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

When the **bgp advertise-map** and **neighbor route-map out** commands are configured, the two policies take effect. However, the policy configured in the **bgp advertise-map** command has a higher priority than the other one.

Examples

The following example matches sent routes with a route map named MAP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp advertise-map MAP
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.14 bgp always-compare-med

Function

Run the **bgp always-compare-med** command to enable the Multi Exit Discriminator (MED) comparison function of BGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The MED comparison function is disabled by default.

Syntax

bgp always-compare-med

no bgp always-compare-med

default bgp always-compare-med

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

Only MED values of paths of peers from the same AS are compared by default. You can run this command to force devices to compare MED values of different AS paths. If there are multiple valid paths to the same destination address, the path with a smaller MED value has a higher priority.

This command is not recommended unless different ASs in the network use the same IGP and route selection methods.

Examples

The following example compares MED attributes during BGP route calculation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp always-compare-med
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 bgp asnotation dot

Function

Run the **bgp asnotation dot** command to display 4-byte AS numbers in dot mode and match regular expressions. Two decimals are separated by dot, for example 65535.65535.

Run the **no** form of this command to configure BGP to display 4-byte AS numbers in decimal notation mode.

Run the **default** form of this command to restore the default configuration.

AS numbers are expressed in decimal notation mode by default.

Syntax

bgp asnotation dot

no bgp asnotation dot

default bgp asnotation dot

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

4-byte AS numbers support two expression modes: decimal notation mode and dot mode. The decimal notation mode is the same as the original expression mode, that is, the 4 bytes of an AS number are expressed in decimal notation. The conversion between the dot mode and decimal notation mode is as follows: 4-byte decimal AS number = x * 65536 + Y. For example:

- For an AS number 65534 in decimal mode, it is 65,534 in dot mode. An AS number smaller than 65536 is the same in decimal mode and dot mode.
- For an AS number 65536 in decimal mode, it is 1.0 in dot mode.
- For an AS number 65538 in decimal mode, it is 1.2 in dot mode.

The display mode of 4-byte AS numbers does not affect the expression mode of the 4-byte AS numbers in BGP commands. The decimal notation and dot modes are supported in BGP commands. The display mode of 4-byte AS numbers in a regular expression must be consistent with the current display mode. Otherwise, the regular expression cannot be matched.

After this command is configured, you must run the **clear ip bgp *** command to reset peers and match regular expressions again according to filtering conditions.

Examples

The following example displays 4-byte AS numbers in dot mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp asnotation dot
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **clear ip bgp**

1.16 bgp bestpath aigp ignore

Function

Run the **bgp bestpath aigp ignore** command to disable AIGP metric value comparison when the optimal path is selected.

Run the **no** form of this command to enable AIGP metric value comparison when the optimal path is selected.

Run the **default** form of this command to restore the default configuration.

The AIGP metric value is compared by default when the optimal path is selected.

Syntax

bgp bestpath aigp ignore

no bgp bestpath aigp ignore

default bgp bestpath aigp ignore

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

The AIGP metric value is compared when the optimal path is selected. The route with a smaller value has a higher priority.

Examples

The following example does not compare AIGP metric values during BGP route calculation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath aigp ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 bgp bestpath as-path ignore

Function

Run the **bgp bestpath as-path ignore** command to not compare AS path length when the optimal path is selected.

Run the **no** form of this command to compare AS path length when the optimal path is selected.

Run the **default** form of this command to restore the default configuration.

The AS path length is compared by default when the optimal path is selected.

Syntax

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

default bgp bestpath as-path ignore

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

The AS path length is compared when the optimal path is selected. The router with a shorter length has a higher priority.

Examples

The following example disables AS path length comparison when the optimal path is selected.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath as-path ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 bgp bestpath as-path multipath-relax

Function

Run the **bgp bestpath as-path multipath-relax** command to enable AS-PATH loose comparison of multiple paths in load balancing mode for BGP.

Run the **no** form of this command to enable AS-PATH precise comparison of multiple paths in load balancing mode for BGP.

Run the **default** form of this command to restore the default configuration.

AS-PATH loose comparison of multiple paths in load balancing mode is not configured for BGP by default.

Syntax

bgp bestpath as-path multipath-relax

no bgp bestpath as-path multipath-relax

default bgp bestpath as-path multipath-relax

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

BGP must accurately compare AS-PATH attributes by default while selecting equal-cost multipath. Equal-cost multipath can be selected only when the AS-PATH attribute is identical. As a result, load balancing cannot be implemented for the paths. After AS-PATH loose comparison is enabled, load balancing can be implemented for multiple paths if the AS-PATH length is compared.

Examples

The following example enables AS-PATH loose comparison for multiple paths in load balancing mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath as-path multipath-relax
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 bgp bestpath compare-confed-aspath

Function

Run the **bgp bestpath compare-confed-aspath** command to compare AS path length when the optimal path is selected.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The AS-PATH attributes of internal EBGP routes from an alliance are not compared by default when the optimal path is selected. Routes are selected based on other conditions.

Syntax

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

default bgp bestpath compare-confed-aspath

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

When the same routes learned from EBGP neighbors in an alliance are selected, the AS path length is not compared by default. After this command is run, a device compares AS path length during route selection. The route with a shorter AS path has a higher priority.

If a route is not configured with the AS-PATH attribute, the device cannot compare the AS path length of this route.

Examples

The following example compares AS path length when the optimal path is selected.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath compare-confed-aspath
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 bgp bestpath compare-routerid

Function

Run the **bgp bestpath compare-routerid** command to compare path router IDs when the optimal path is selected.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

During selection of the optimal path, if two paths with the same path attributes are received from different EBGP peers, the first received path is the optimal path by default.

Syntax

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

default bgp bestpath compare-routerid

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

During selection of the optimal path, if two paths with the same path attributes are received from different EBGP peers, the first received path is the optimal path by default. You can configure this command to select the path with the smallest router ID as the optimal path.

Examples

The following example compares Router IDs of paths when the optimal path is selected.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath compare-routerid
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 bgp bestpath igp-metric ignore

Function

Run the **bgp bestpath igp-metric ignore** command to not compare the next-hop IGP metric values when the optimal path is selected.

Run the **no** form of this command to compare the next-hop IGP metric values when the optimal path is selected.

Run the **default** form of this command to restore the default configuration.

The next-hop IGP metric values are compared by default when the optimal path is selected.

Syntax

bgp bestpath igp-metric ignore

no bgp bestpath igp-metric ignore

default bgp bestpath igp-metric ignore

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

A device compares the next-hop IGP metric values when it selects the optimal path. The route with a smaller value has a higher priority.

Examples

The following example does not compare next-hop IGP metric values during BGP route calculation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath igp-metric ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 bgp bestpath med confed

Function

Run the **bgp bestpath med confed** command to compare path MED values from the same AS alliance when the optimal path is selected.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of comparing path MED values from the same AS alliance is not enabled by default when the optimal path is selected.

Syntax

bgp bestpath med confed [**missing-as-worst**]

no bgp bestpath med confed [**missing**-**as**-**worst**]

default bgp bestpath med confed [**missing**-**as**-**worst**]

Parameter Description

missing-as-worst: Sets the priority of a path without the MED attribute to the lowest level. If this parameter is not specified, the path without the MED attribute has a lower priority.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

When a device compares path attributes, the path with a smaller MED value has a higher priority.

Examples

The following example compares the path MED values of peers from the same AS alliance when the optimal path is selected.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath med confed
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 bgp bestpath med missing-as-worst

Function

Run the **bgp bestpath med missing-as-worst** command to set the priority of a path without the MED attribute to the lowest level when the optimal path is selected.

Run the **no** form of this command to set the priority of a path without the MED attribute to the highest level when the optimal path is selected.

Run the **default** form of this command to restore the default configuration.

The priority of a path without the MED attribute is set to the highest level by default when the optimal path is selected.

Syntax

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

default bgp bestpath med missing-as-worst

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

When a device compares path attributes, the path with a smaller MED value has a higher priority.

Examples

The following example sets the priority of a path without the MED attribute to the lowest level when the optimal path is selected.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65530
Hostname(config-router)# bgp bestpath med missing-as-worst
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 bgp bestpath multipath-compare-routerid

Function

Run the **bgp bestpath multipath-compare-routerid** command to enable the function of comparing router IDs of multiple paths in load balancing mode.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of comparing router IDs of multiple paths in load balancing mode is disabled by default.

Syntax

bgp bestpath multipath-compare-routerid

no bgp bestpath multipath-compare-routerid

default bgp bestpath multipath-compare-routerid

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

When a device receives multiple pieces of routing information from the same router ID, load balancing can be implemented for the routes.

Examples

The following example compares router IDs of multiple paths in load balancing mode of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bestpath multipath-compare-routerid
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 bgp bmp-active

Function

Run the **bgp bmp-active** command to enable all BMP servers to monitor all BGP neighbors.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of enabling all BMP servers to monitor all neighbors is disabled by default.

Syntax

bgp bmp-active

no bgp bmp-active

default bgp bmp-active

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables all BGP servers to monitor all neighbors in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp bmp-active
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 bgp client-to-client reflection

Function

Run the **bgp client-to-client reflection** command to enable the route reflection function between device clients.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The route reflection function between clients is enabled by default.

Syntax

bgp client-to-client reflection

no bgp client-to-client reflection

default bgp client-to-client reflection

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

Generally, you do not need to create connections between the clients of a route reflector because the route reflector can reflect the routes between the clients. If a full mesh of connections is established among all clients, you can cancel the function of client route reflection of the route reflector.

Examples

The following example disables the route reflection function between clients of a device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# no bgp client-to-client reflection
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 bgp cluster-id

Function

Run the **bgp cluster-id** command to configure the cluster ID for a route reflector.

Run the **no** form of this command to configure BGP to use a local router ID as the cluster ID.

Run the **default** form of this command to restore the default configuration.

The cluster ID of a route reflector is used as the route ID of the route reflector by default.

Syntax

bgp cluster-id [*cluster-id* | *ipv4-address*]

no bgp cluster-id

default bgp cluster-id

Parameter Description

cluster-id: Cluster ID of a route reflector. The value range is from 1 to 4294967295.

ipv4-address: Cluster ID of a route reflector.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

Generally, only one route reflector is configured in a cluster. In this case, you can use the router ID of the route reflector to identify this cluster. To increase reliability, you can configure multiple route reflectors in a cluster. In this case, you must configure the cluster ID to ensure that the route reflector can identify route update messages from other route reflectors in the cluster.

Examples

The following example configures the cluster ID of a route reflector as 10.0.0.1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp cluster-id 10.0.0.1
```

Notifications

If the entered cluster ID is invalid, the following notification will be displayed:

```
% Invalid cluster-id
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 bgp confederation identifier

Function

Run the **bgp confederation identifier** command to configure an ID for an AS alliance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ID is configured for an AS alliance of BGP by default.

Syntax

bgp confederation identifier *as-number*

no bgp confederation identifier

default bgp confederation identifier

Parameter Description

as-number: ID of an AS alliance. The value range is from 1 to 65535. A device can be configured with a 4-byte AS number. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

An alliance is method of reducing the IBGP peer connections within an AS.

An AS is divided into multiple sub ASs and configured with a unified alliance ID (namely, AS number) for these sub ASs to form an alliance. Outside the alliance, the entire alliance is still considered as an AS and only the AS number of the alliance is visible. Inside the alliance, a full mesh of IBGP peers is established for BGP speakers

within a sub AS, and EBGP peer connections are established for BGP speakers in different sub ASs. Though EBGP connections are established between BGP speakers in different sub ASs, the next hop, MED, local priority and other information keep unchanged when information is exchanged.

Examples

The following example sets the ID of an AS alliance to **65000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp confederation identifier 65000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 bgp confederation peers

Function

Run the **bgp confederation peers** command to configure a member AS for an AS alliance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No member AS is configured for an AS alliance by default.

Syntax

bgp confederation peers *as-number*&<1-n>

no bgp confederation peers *as-number*&<1-n>

default bgp confederation peers *as-number*&<1-n>

Parameter Description

as-number&<1-n>: Member AS within an alliance. A 4-byte AS number can be configured. That is, the AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode. & <1-n> specifies that 1 to *n* members ASs can be configured for an alliance.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

An alliance is method of reducing the IBGP peer connections within an AS.

An AS is divided into multiple sub ASs and configured with a unified alliance ID (namely, AS number) for these sub ASs to form an alliance. Outside the alliance, the entire alliance is still considered as an AS and only the AS number of the alliance is visible. Inside the alliance, a full mesh of IBGP peers is established for BGP speakers within a sub AS, and EBGP peer connections are established for BGP speakers in different sub ASs. Though EBGP connections are established between BGP speakers in different sub ASs, the next hop, MED, local priority and other information keep unchanged when information is exchanged.

Examples

The following example configures members ASs 65000 and 65100 for an alliance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp confederation peers 65000 65100
```

Notifications

If the entered member AS number is consistent with the local AS number, the following notification will be displayed:

```
% Local member-AS not allowed in confed peer list
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 bgp dampening

Function

Run the **bgp dampening** command to enable the route dampening function and configure dampening parameters.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The route dampening function is disabled by default.

Syntax

bgp dampening [*half-life* [*reusing suppressing maximun-supress-time*] [**withdrawal-ignore**] | **route-map** *route-map-name*]

no bgp dampening

default bgp dampening

Parameter Description

half-life: Half life time. When the life time in minutes reaches this value, the penalty is halved. The value range is from 1 to 45, and the default value is **15**.

reusing: Reuse Limit. When the penalty is reduced to this value, the route is activated again. The value range is from 1 to 10000, and the default value is **750**.

suppressing: Suppress limit. When the penalty is greater than this value, the route is suppressed. The value range is from 1 to 20000, and the default value is **2000**.

maximun-supress-time: Maximum time of route suppression. When the time in minutes exceeds this value, the route is activated. The value range is from 1 to 255, and the default value is **60**.

withdrawal-ignore: Specifies that the penalty does not increase when the route is activated again.

route-map *route-map-name*: Calls a route map to apply the route dampening function to a specific route. Route dampening is applied to all routes by default.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to suppress unstable EBGP routes and does not apply to IBGP routes.

Penalty is used to describe route stability. A greater penalty indicates a more unstable route. The penalty increases by 1000 each time route flapping occurs once (a withdraw packet is received). The penalty does not increase after it reaches a value. This value is called the upper limit of penalty. The value is subject to the configured *maximun-supress-time*. The formula is as follows: Upper limit of penalty = 2 ^ (*maximun-supress-time*/*half-life*) * *reusing.* Because the upper limit of penalty cannot exceed 20000, the values of *maximun-supress-time*, *half-life*, and *reusing* must be adjusted based on the network status.

1. Relationship between *Half-time and maximun-supress-time*: *half-time* ≤ *maximum-supress-time*

2. Relationship between *reusing*, *suppressing*, and upper limit of penalty: *reusing* ≤ *suppressing* ≤ upper limit of penalty

Users can specify only the *half-life* value. In this case, the value of *maximun-supress-time* is (*half-life* × 4), and the values of *reusing* and *suppressing* are 750 and 2000 respectively.

If the penalty of an EBGP route exceeds the value of *suppressing*, the route is suppressed. A suppressed route is neither used during BGP route selection nor advertised to other BGP peers. If the suppressed routes go on flapping, the penalty rises to the upper limit of penalty.

If the *half-life* of a suppressed route passes, the penalty is halved. If the penalty decreases to the value of *reusing*, the route of update packets is selected by BGP again at the last update. If the penalty decreases to the value 0, the route of withdraw packets is removed from the BGP routing table at the last update.

By default, the penalty value increases by 1000 when a route is reactivated and increases by 500 when a route is updated.

Route suppression information is recalculated during active/standby switchover in the Virtual Switching Unit (VSU) environment.

Examples

The following example sets the **Half-life-time** to **30** minutes, **Reuse Limit** to **1200**, **Suppress Limit** to **10000**, and **Max-suppress-time** to **120** minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp dampening 30 1200 10000 120
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

If configuration is completed in the scope VRF mode and the IPv6 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv6 unicast of vrf vrf-name enabled.
```

If the configured **maximun-supress-time** value is smaller than the **Half-life-time** value, the following notification will be displayed:

```
% Maximum suppress time cannot be less than half life time.
```

If the configured **Suppress Limit** value is smaller than the **Reuse Limit** value, the following notification will be displayed:

```
% Suppress value cannot be less than reuse value.
```

If the upper limit of the penalty obtained based on the configured parameters is greater than 10000, the following notification will be displayed:

```
% Either maximun-supress-time time or reusing value is too large.
```

If the upper limit of the penalty obtained based on the configured parameters is smaller than the **Suppress Limit** value, the following notification will be displayed:

```
% Either maximun-supress-time time or reusing value is too small.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 bgp default ipv4-unicast

Function

Run the **bgp default ipv4-unicast** command to configure the default address family as the IPv4 unicast address family.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default address family by default is the IPv4 unicast address family.

Syntax

bgp default ipv4-unicast

no bgp default ipv4-unicast

default bgp default ipv4-unicast

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the default address family as the IPv4 unicast address family.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp default ipv4-unicast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 bgp default local-preference

Function

Run the **bgp default local-preference** command to configure the default LOCAL_PREF attribute.

Run the **no** form of this command to restore the default LOCAL_PREF attribute.

Run the **default** form of this command to restore the default configuration.

The default LOCAL_PREF value is **100**.

Syntax

bgp default local-preference *local-preference-value*

no bgp default local-preference

default bgp default local-preference

Parameter Description

local-preference-value: Attribute value of a local priority. The value range is from 0 to 4294967295, and the default value is **100**.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

BGP uses the LOCAL_PREF attribute as a basis for comparing priorities of paths learned from IBGP peers. A path with a larger LOCAL_PREF value has a higher priority.

When sending external routes to IBGP peers, a BGP speaker adds the LOCAL_PREF attribute.

Examples

The following example sets the default LOCAL_PREF value to **200**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp default local-preference 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 bgp default route-target filter

Function

Run the **bgp default route-target filter** command to enable the Route-Target filtering function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The Route-Target filtering function is enabled by default.

Syntax

bgp default route-target filter

no bgp default route-target filter

default bgp default route-target filter

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

After the **no bgp default route-target filter** command is run, BGP receives all VPN routes whether the Route-Target of the local VRF instance is filtered or not.

When a PE route reflector client is configured for BGP, the device receives all VPN routes, regardless of the configuration of this command.

Examples

The following example disables the Route-Target filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# no bgp default route-target filter
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 bgp deterministic-med

Function

Run the **bgp deterministic-med** command to preferentially compare path MED values for peers from the same AS.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Path MED values for peers from the same AS are not compared by default.

Syntax

bgp deterministic-med

no bgp deterministic-med

default bgp deterministic-med

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

By default, a device compares path MED values based on the sequence of the received paths by default when the optimal path is selected.

Examples

The following example preferentially compares path MED values for peers from the same AS.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp deterministic-med
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 bgp dmzlink-bw

Function

Run the **bgp dmzlink-bw** command to advertise bandwidth of a specified interface as an extended attribute.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No bandwidth of a specified interface is advertised as an extended attribute.

Syntax

bgp dmzlink-bw

no bgp dmzlink-bw

default bgp dmzlink-bw

Parameter Description

N/A

Command Modes

BGP configuration mode

IPv4 unicast address family mode of BGP

IPv6 unicast address family mode of BGP

IPv4 VRF address family mode of BGP

IPv6 VRF address family mode of BGP

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to configure links for directly connected EBGP peers. After the **neighbor send-community** command is configured, the extended community attribute of link bandwidth is transmitted to IBGP peers. This command is used with the **maximum-paths { ebgp | ibgp }** *maximum-paths-number* command to configure load balancing for multiple paths on links with unequal bandwidth. This command takes effect only when each directly connected EBGP peer carries the extended community attribute of link bandwidth.

Examples

The following example advertises the bandwidth of a specified interface as an extended attribute in the IPv4 address family.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# address-family ipv4
Hostname(config-router-af)# bgp dmzlink-bw
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 bgp enforce-first-as

Function

Run the **bgp enforce-first-as** command to configure a device to check the first AS number of the AS_PATH field in update packets.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

A device checks the first AS number of the AS_PATH field in update packets by default.

Syntax

bgp enforce-first-as

no bgp enforce-first-as

default bgp enforce-first-as

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

A device obtains routing information by receiving update packets. When the device attempts to advertise the routing information learned from the update packets to other devices:

- If the routing information is advertised to EBGP peers, the device adds the local AS number to the AS_PATH field as the first AS number. The EBGP peers can know the ASs that the packets need to pass before they reach the destination address based on the AS_PATH attribute in this routing information.
- If the routing information is advertised to IBGP peers, the AS_PATH attribute remains unchanged.

After this command is configured, the device determines the first AS number of the AS_PATH attribute in update packets when it receives the update packets from EBGP peers. If the first AS number is not the AS number of the EBGP peers, the packets are directly discarded.

Examples

The following example configures a device to check the first AS number of the AS_PATH field in update packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp enforce-first-as
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 bgp fast-external-fallover

Function

Run the **bgp fast-external-fallover** command to enable the fast link detection function of EBGP neighbors.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The fast link detection function of EBGP neighbors is enabled by default.

Syntax

bgp fast-external-fallover

no bgp fast-external-fallover

default bgp fast-external-fallover

Parameter Description

N/A

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

This command is effective to only directly connected EBGP peers. After this command is configured, the BGP session connection is disabled immediately if the network interface used to establish a connection with the directly connected EBGP neighbors fails.

Examples

The following example enables the fast link detection function of EBGP neighbors.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp fast-external-fallover
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 bgp fast-reroute

Function

Run the **bgp fast-reroute** command to enable the fast rerouting (FRR) function of BGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The FRR function is disabled by default.

Syntax

bgp fast-reroute

no bgp fast-reroute

default bgp fast-reroute

Parameter Description

N/A

Command Modes

BGP configuration mode

IPv4 unicast address family mode of BGP

IPv6 unicast address family mode of BGP

IPv4 VRF address family of BGP

IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The FRR function of BGP is restricted by the following:

- Only one backup route is generated and the next hop of the backup route cannot be the same as that of the preferred route.
- A backup next hop cannot be generated for an Equal-Cost Multi-Path Routing (ECMP) route.
- The FRR function of BGP has a lower priority than that of VPN. That is, if VPN FRR is enabled in the VRF mode, the FRR function of BGP can take effect only when VPN FRR fails to calculate a backup route.
- This command and the **bgp install standby-path** command cannot be configured concurrently.

Examples

The following example enables the FRR function of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65530
Hostanme(config-router)# bgp fast-reroute
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 bgp fast-withdraw

Function

Run the **bgp fast-withdraw** command to enable the fast withdrawal function of a specified BGP route.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The fast withdrawal function for a specified BGP route is disabled by default.

Syntax

bgp fast-withdraw { **access-list** { *access-list-number* | *access-list-name* } | **prefix-list** *prefix-list-name* | **route-map** *route-map-name* }

no bgp fast-withdraw { **access-list** | **prefix-list** | **route-map** }

default bgp fast-withdraw { **access-list** | **prefix-list** | **route-map** }

Parameter Description

access-list-number: Number of an Access Control List (ACL). The value range is from 1 to 199 or from 1300 to 2699.

access-list-name: Name of an ACL.

prefix-list-name: Name of a prefix list.

route-map-name: Name of a matched route map rule.

Command Modes

BGP configuration mode

IPv4 unicast address family mode of BGP

IPv6 unicast address family mode of BGP

IPv4 VRF address family of BGP

IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The fast withdrawal function of a specified BGP route is restricted by the following:

- Either the **prefix-list** or **access-list** keyword takes effect.

Examples

The following example enables the fast withdrawal function of a specified BGP route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostanme(config-router)# bgp fast-withdraw route-map bgp-filter
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 bgp graceful-restart

Function

Run the **bgp graceful-restart** command to enable the function of global BGP graceful restart (GR).

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of global BGP GR is enabled by default.

Syntax

bgp graceful-restart

no bgp graceful-restart

default bgp graceful-restart

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

BGP GR enables a device to keep the BGP routing table valid and continue to forward data during restart. After this command is configured, the device can execute GR or help neighbors execute GR.

The BGP GR capability is advertised through the capability field in an open message and negotiated in the initial establishment of connections between a device and its peer. Both the device and its peer must support the GR capability. If neither of them support GR, the route device does not correctly implement GR.

After this command is configured, it does not take effect to all established BGP connections. Therefore, to negotiate immediately about the GR capability on these BGP connections, forcibly restart the BGP connections to renegotiate about GR capability between the local device and its peer. You can run the **clear ip bgp** command to restart the BGP connections between peers.

BGP detects neighbor GR based on TCP failure messages. If a TCP failure occurs in non-GR scenario, for example, the **shutdown** command is run in interface configuration mode, BGP enters the GR Helper state and retains neighbor routes, and converges the routes after GR times out or a connection with the neighbor is reestablished.

Examples

The following example enables the global BGP GR function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostanme(config-router)# bgp graceful-restart
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 bgp graceful-restart disable

Function

Run the **bgp graceful-restart disable** command to disable the GR function of a specified BGP address family.

Run the **no** form of this command to enable the GR function of a specified BGP address family.

Run the **default** form of this command to restore the default configuration.

When the global BGP GR function is enabled, the GR function of each BGP address family is enabled by default.

Syntax

bgp graceful-restart disable

no bgp graceful-restart disable

default bgp graceful-restart disable

Parameter Description

N/A

Command Modes

BGP configuration mode

IPv4 unicast address family mode of BGP

IPv4 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

When the BGP GR function is enabled, this activates the GP capability of address families by default, except those that do not support GR. You can run this command in address family configuration mode to disable the GR capability of the specified address family. If this command is configured in BGP mode, it acts on IPv4 unicast address families.

When the BGP GR function is disabled, the GR capability of all address families is disabled.

Examples

The following example disables the GR capability of the IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostanme(config-router)# bgp graceful-restart
Hostanme(config-router)# address-family ipv4
Hostanme(config-router-af)# bgp graceful-restart disable
```

Notifications

If the GR capability is not supported in the current address family, the following notification will be displayed:

```
% The address family does not support graceful restart
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 bgp graceful-restart restart-time

Function

Run the **bgp graceful-restart restart-time** command to configure the GR time of BGP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The GR time is **120** seconds by default.

Syntax

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time

default bgp graceful-restart restart-time

Parameter Description

restart-time: Expected maximum wait time before the establishment of a connection between the GR Helper and the GR Restarter, in seconds. The value range is from 1 to 3600.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

The restart time is advertised by the GR Restarter to the GR Helper, which indicates the expected maximum wait time before the establishment of a connection between the GR Helper and the GR Restarter. If no BGP connection is established between the GR Helper and GR Restarter after this timer expires, the BGP connection request fails. A normal BGP restart process is performed. During this process, all routes of this neighbor are deleted and data forwarding is affected.

This value is advertised in the GR capability field of the Open message of BGP. You are advised to configure the same GR restart time for the devices at both ends of a session.

This command does not take immediately effect to all established BGP connections. Therefore, you must forcibly disconnect and reestablish the BGP connections to renegotiate the GR capability and advertise the latest restart time to the GR Helper. You can run the **clear ip bgp** command to forcibly disconnect and reestablish a BGP connection. The configured restart time should not be greater than the Hold Time of the BGP peer; otherwise, the Hold Time is used as the restart time and advertised to the BGP peer during GR capability advertisement.

Examples

The following example sets the GR time of BGP to **150** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostanme(config-router)# bgp graceful-restart
Hostanme(config-router)# bgp graceful-restart restart-time 150
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 bgp graceful-restart stalepath-time

Function

Run the **bgp graceful-restart stalepath-time** command to configure the hold time of a stale route by a GR Helper during BGP GR.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default hold time of a stale route by a GR Helper during BGP GR is **360** seconds.

Syntax

bgp graceful-restart stalepath-time *stalepath-time*

no bgp graceful-restart stalepath-time

default bgp graceful-restart stalepath-time

Parameter Description

stalepath-time: Maximum hold time in seconds of a stale route after a connection with a GR device is recovered. The value range is from 1 to 3600.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

This command applies to GR Helpers.

StalePath-time specifies the maximum wait time of the EOR flag from the GR Restarter after a connection is recovered between the GR Helper and the GR Restarter. Upon detecting the disconnection from the GR Restarter, the GR Helper marks the original routes to the GR Restarter as Stale, but uses these routes to calculate and forward routes. The GR Helper updates route information based on the route update message received from the GR Restarter and removes the Stale mark from the routes. In the stalepath-time, the stale routes are deleted if they are not updated. This mechanism is used to ensure route convergence if the GR Helper does not receive the EOR flag for a long time.

Examples

The following example sets the hold time of a stale route by a GR Helper during BGP GR to **240** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostanme(config-router)# bgp graceful-restart
Hostanme(config-router)# bgp graceful-restart stalepath-time 240
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 bgp initial-advertise-delay

Function

Run the **bgp initial-advertise-delay** command to enable the function of BGP delayed advertisement upon system restart.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of BGP delayed advertisement upon system restart is disabled by default.

Syntax

bgp initial-advertise-delay { *delay-time* [*startup-time*] [**wait-for-controller**] | **prefix-list** *prefix-list-name* }

no bgp initial-advertise-delay [**prefix-list**]

default bgp initial-advertise-delay [**prefix-list**]

Parameter Description

delay-time: Interval in seconds of route advertisement after the BGP neighborship is established upon system restart. The value range is from 1 to 1800, and the default value is **1**.

startup-time: Time range in seconds for system restart. In this range, neighbors use the delayed advertisement mechanism of routes. The value range is from 5 to 58400, and the default value is **600**.

wait-for-controller: Waits for the controller to deliver messages and triggers route advertisement.

prefix-list: Immediately sends routes that match the prefix list upon system restart.

prefix-list-name: Name of a prefix list. The name does not exceed 255 characters.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

Users can adjust the BGP route advertisement upon system restart according to the hardware conditions, neighbor number, route number, and deployment requirements of devices.

Generally, after a connection is established between the local device and its neighbor, a first route is advertised immediately, and later routes are advertised at the default interval (for details, see the **bgp additional-paths select**

- **neighbor additional-paths**

neighbor advertisement-interval command). This command can modify BGP peers to advertise routes to neighbors upon system restart. After this command is configured, BGP advertises routes to neighbors at an interval *delay-time* within the *startup-time* of the device after system restart.

If the **wait-for-controller** keyword is configured, the device waits for the controller to deliver route advertisement messages and trigger route advertisement upon receiving EOR messages from neighbors. In the *startup-time*, if no message is received, routes are sent forcibly.

After this command is configured, routes that are advertised at a normal interval are affected. You can specify the **prefix-list** parameter to prevent routes that match the prefix list from being affected by the delayed advertisement mechanism and send the routes at the default interval. For the range of address families applicable to the prefix list, see the **neighbor pic-disable** command.

Examples

The following example configures BGP to send routes at an interval of 60 seconds within 500 seconds upon system restart, and to send routes that match the prefix list aa at a normal interval.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostanme(config-router)# bgp initial-advertise-delay 60 500
Hostanme(config-router)# bgp initial-advertise-delay prefix-list aa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bgp additional-paths select**
- **neighbor additional-paths**
- neighbor advertisement-interval
- **neighbor prefix-list**

1.45 bgp install standby-path

Function

Run the **bgp install standby-path** command to enable the function of standby path installation of BGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of standby path installation is disabled by default.

Syntax

bgp install standby-path

no bgp install standby-path

default bgp install standby-path

Parameter Description

N/A

Command Modes

BGP configuration mode

IPv4 unicast address family mode of BGP

IPv6 unicast address family mode of BGP

IPv4 VRF address family of BGP

IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This function and the FRR function of BGP cannot be enabled concurrently.

Examples

The following example enables the function of standby path installation of BGP.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostanme(config-router)# bgp install standby-path
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 bgp link-state-group up-delay

Function

Run the **bgp link-state-group up-delay** command to configure the delay time to unbind the downlink port in the link state tracking group associated with the BGP neighbors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default delay time to unbind the downlink port in the link state tracking group associated with the BGP neighbors is **5** seconds.

Syntax

bgp link-state-group up-delay *delay-time*

no bgp link-state-group up-delay

default bgp link-state-group up-delay

Parameter Description

delay-time: Delay time in seconds to unbind the downlink port in the link state tracking group associated with the BGP neighbors. The value range is from 1 to 30.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the default delay time to unbind the downlink port in the link state tracking group associated with the BGP neighbors to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostname(config-router)# bgp link-state-group up-delay 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 bgp log-neighbor-changes

Function

Run the **bgp log-neighbor-changes** command to configure a device to record BGP state changes without enabling the debugging function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

A device records the BGP state changes without enabling the debugging function by default.

Syntax

bgp log-neighbor-changes

no bgp log-neighbor-changes

default bgp log-neighbor-changes

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

You can run the **debug bgp** command to record BGP state changes but consumes many device resources. You are advised to configure this command to record BGP state changes.

Examples

The following example records BGP state changes without enabling the debugging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostname(config-router)# bgp log-neighbor-changes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.48 bgp maxas-limit

Function

Run the **bgp maxas-limit** command to limit the quantity of AS numbers in the AS_PATH attribute for BGP routes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The quantity of AS numbers in the AS_PATH attribute for routes is not limited by default.

Syntax

bgp maxas-limit *maxas-limit-number*

no bgp maxas-limit

default bgp maxas-limit

Parameter Description

maxas-limit-number: Maximum quantity of AS numbers carried in the AS_PATH attribute. The value range is from 1 to 512.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, this routing information is discarded if the quantity of AS numbers in the AS_PATH attribute in the routing information received from a peer exceeds the specified upper threshold.

After you change the configuration, you must manually run the **clear ip bgp** command to reset neighbors so as to validate the command.

Examples

The following example sets the maximum allowable quantity of AS numbers in the AS_PATH attribute for a BGP route to **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp maxas-limit 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 bgp maximum-neighbor

Function

Run the **bgp maximum-neighbor** command to configure the maximum number of BGP neighbors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of neighbors is not configured by default.

Syntax

bgp maximum-neighbor *maximum-neighbor-numbers* **warning-only**

no bgp maximum-neighbor

default bgp maximum-neighbor

Parameter Description

maximum-neighbor-numbers: Maximum number of neighbors. The value range is from 1 to 15000.

warning-only: Gives an alarm only.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Usage Guidelines

When the number of BGP neighbors exceeds the specified maximum value, the device gives an alarm.

Examples

The following example sets the maximum number of BGP neighbors to **1000** in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp maximum-neighbor 1000 warning-only
```

Related Commands

N/A

Notifications

N/A

Usage Guidelines

N/A

Platform Description

N/A

1.50 bgp maximum-prefix

Function

Run the **bgp maximum-prefix** command to configure the maximum number of route entries in global configuration mode or for specified VRF instances.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The function of route entry limit is disabled in global configuration mode or for specified VRF instances by default.

Syntax

bgp maximum-prefix *maximum-prefix-numbers* [**vrf** *vrf-name*]

no bgp maximum-prefix [**vrf** *vrf-name*]

default bgp maximum-prefix [**vrf** *vrf-name*]

Parameter Description

maximum-neighbor-numbers: Maximum number of route entries. The value range is from 1 to 4294967295.

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, the route entry limit function is enabled in global configuration mode.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Usage Guidelines

The prefix information of BGP routes may be imported by configuring the **redistribute** command, learned from neighbors, or imported from other VRF instances. In any scenario, if the imported prefix information of BGP routes in an address family enables the routes in global configuration mode or for specified VRF instances to reach the upper limit, the route prefix information of this address family is not added. In this case, the table of this address family and all neighbors in this address family enters the overflow state. In this case, the device prompts that BGP enters the overflow state in global configuration mode or for specified VRF instances.

You can run the **show bgp** { *address-family* | **all** } **summary** command to display the state of the routing information base.

To clear this state, you need to reconfigure BGP or run the **clear bgp** *address-family* ***** command to reset the address family. If the address family enters the overflow state because the prefix information of BGP routes reaches the maximum number of entries, you can configure the *maximum-prefix-numbers* parameter to change the setting.

For IPv4 unicast routes, even if the address family reaches the overflow state, route prefixes may be received in the following scenarios:

- The routing information with same prefixes is configured in the routing information base.
- A route overwriting the prefix (except for the default route) is configured in the routing information base and the next hop of this route is different from that of the newly received route.

Examples

The following example sets the maximum number of prefixes of BGP routes to **100** in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp maximum-prefix 100
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 bgp mp-error-handle session-retain

Function

Run the **bgp mp-error-handle session-retain** command to configure BGP to retain BGP sessions when it detects a multiprotocol route error.

Run the **no** form of this command to configure BGP to terminate BGP sessions when it detects a multiprotocol route error.

Run the **default** form of this command to restore the default configuration.

BGP terminates BGP sessions by default when it detects a multiprotocol route error.

Syntax

bgp mp-error-handle session-retain [**refresh-timer** *refresh-timer*]

no bgp mp-error-handle session-retain

default bgp mp-error-handle session-retain

Parameter Description

refresh-timer *refresh-timer*: Configures the wait time in seconds for automatic route recovery. The value range is from 10 to 65535, and the default value is **120**.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

Upon receiving Update packets from a neighbor, the device terminates the BGP session if it detects a multiprotocol route error. This will cause flapping of the routes in all address families of this neighbor. That is, the routing error in an address family affects the route stability in other address families. After this command is configured, only the routing information related to this address family is deleted, and BGP sessions and other address families are not affected if an error occurs in the routing attribute of an address family. This enhances the stability of BGP.

You can specify the **refresh-timer** keyword to configure the wait time for automatic route recovery. But a neighbor must support the route-refresh capability. After the *refresh-timer* times out, BGP sends the route update messages of the address family to the neighbor and re-advertises all routing information of the address family to this neighbor. If the **refresh-timer** keyword is not specified during the command configuration, the default value is **120** seconds.

Examples

The following example configures BGP to retain BGP sessions when it detects a multiprotocol route error.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router bgp 100
Hostname(config-router)# bgp mp-error-handle session-retain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 bgp nexthop trigger delay

Function

Run the **bgp nexthop trigger delay** command to configure a delay of updating the routing table after the next hop of a BGP route changes.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default delay of updating the routing table is **5** seconds after the next hop of a BGP route changes.

Syntax

bgp nexthop trigger delay *delay-time*

no bgp nexthop trigger delay

default bgp nexthop trigger delay

Parameter Description

delay-time: Delay in seconds of updating the routing table after the next hop of a BGP route changes. The value range is from 0 to 100.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command can take effect only when the **bgp nexthop trigger enable** command is configured.

Examples

The following example sets the delay of updating the routing table to **30** seconds after the next hop of a BGP route changes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp nexthop trigger delay 30
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

If the function of next hop trigger update is disabled, the following notification will be displayed:

```
% Can't disable scan-rib, please enable nexthop trigger first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bgp nexthop trigger enable**

1.53 bgp nexthop trigger enable

Function

Run the **bgp nexthop trigger enable** command to enable the function of next hop trigger update.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of next hop trigger update is enabled by default.

Syntax

bgp nexthop trigger enable

no bgp nexthop trigger enable

default bgp nexthop trigger enable

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

Next hop update of BGP is triggered by events. After this function is enabled, the device notifies BGP of this change when a device updates the next hop in the routing information base (RIB). This shortens the response time of BGP to the next hop change in the RIB routes and improves the overall convergence performance of BGP.

Examples

The following example enables the function of next hop trigger update.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# bgp nexthop trigger enable
```

Notifications

If this function is disabled in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If this function is disabled in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 bgp notify unsupport-capability

Function

Run the **bgp notify unsupport-capability** command to enable the detection function of neighbor address family capability.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The detection function of neighbor address family capability is disabled by default.

Syntax

bgp notify unsupport-capability

no bgp notify unsupport-capability

default bgp notify unsupport-capability

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

If the neighbor address family capability of BGP on the local device is not consistent with that on the neighbor, neighbor connections can still be established by default. After this command is configured, a notification packet carrying the unsupported address family is sent to the neighbor if the address family capability is supported only on the local device.

Examples

The following example enables the detection function of neighbor address family capability of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp notify unsupport-capability
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 bgp nsr

Function

Run the **bgp nsr** command to enable the global non-stop routing (NSR) function of BGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The global NSR function of BGP is disabled by default.

Syntax

bgp nsr

no bgp nsr

default bgp nsr

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, the NSR function for all neighbors is enabled.

Examples

The following example enables the global NSR function of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp nsr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 bgp recursion host

Function

Run the **bgp recursion host** command to enable BGP routes to recurse to only host routes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BGP routes use the optimal matching mode for route recursion by default.

Syntax

bgp recursion host

no bgp recursion host

default bgp recursion host

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is effective to only non-directly-connected BGP routes.

Examples

The following example enables BGP routes to recurse to only host routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp recursion host
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 bgp redistribute-internal

Function

Run the **bgp redistribute-internal** command to configure BGP to allow the routes received from IBGP neighbors to be redistributed to Interior Gateway Protocol (IGP).

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

BGP allows the routes received from IBGP neighbors to be redistributed to IGP.

Syntax

bgp redistribute-internal

no bgp redistribute-internal

default bgp redistribute-internal

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to determine whether to allow IBGP routes to be redistributed to IGP, including Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS).

Examples

The following example allows routes received from IBGP neighbors to be redistributed to IGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp redistribute-internal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 bgp route-reflector attribute-change

Function

Run the **bgp route-reflector attribute-change** command to allow the route reflector to modify route attributes.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No route reflector is allowed to modify route attributes by default.

Syntax

bgp route-reflector attribute-change

no bgp route-reflector attribute-change

default bgp route-reflector attribute-change

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

Generally, the route reflector cannot modify route attributes through routing policies, because this may cause a routing loop. After this command is configured, the route reflector can forcibly modify route attributes through routing policies. This command is used to replan network traffic.

Examples

The following example allows the route reflector to modify route attributes.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp route-reflector attribute-change
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 bgp router-id

Function

Run the **bgp router-id** command to configure a router ID when the BGP is running.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The loopback interface of a device is preferred as the router ID by default. If no loopback interface is available, the router ID of the local device is used.

Syntax

bgp router-id *ipv4-address*

no bgp router-id

default bgp router-id

Parameter Description

ipv4-address: Specified router ID in the format of an IPv4 address.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

The ID of each device in an AS must be unique.

Examples

The following example sets the router ID to 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp router-id 10.0.0.1
```

Notifications

If the entered router ID is invalid, the following notification will be displayed:

```
% Invalid router-id
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 bgp scan-rib disable

Function

Run the **bgp scan-rib disable** command to update the routing table in event triggering mode.

Run the **no** form of this command to update the routing table in regular scanning mode.

Run the **default** form of this command to restore the default configuration.

BGP updates the routing table in regular scanning mode by default.

Syntax

bgp scan-rib disable

no bgp scan-rib disable

default bgp scan-rib disable

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

BGP provides two route update mechanisms: regular-scanning update and event-triggering update.

- Regular-scanning update specifies that BGP updates the routing table based on an internal timer.
- Event-triggering update specifies that BGP updates the routing table when the BGP configuration commands are changed due to user configuration or when the next hop of a BGP route changes.

Examples

The following example configures the routing table update mode as event triggering.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp scan-rib disable
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

If regular scanning is disabled while BGP route synchronization is enabled, the following notification will be displayed:

```
% Can't disable scan-rib, please disable synchronization first
```

If regular scanning is disabled while next hop trigger update is disabled, the following notification will be displayed information:

```
% Can't disable scan-rib, please enable nexthop trigger first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 bgp scan-time

Function

Run the **bgp scan-time** command to configure the interval of regular scanning of BGP.

Run the **no** form of this command to configure the interval of regular scanning of BGP to a default value.

Run the **default** form of this command to restore the default configuration.

The default interval of regular scanning is **60** seconds.

Syntax

bgp scan-time *scan-time*

no bgp scan-time

default bgp scan-time

Parameter Description

scan-time: Interval in seconds of regular scanning. The value range is from 5 to 60.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to configure the interval of regular scanning. The configuration takes effect when the route update mechanism of BGP is configured as regular scanning.

Examples

The following example sets the interval of regular scanning to **30** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp scan-time 30
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 bgp shutdown

Function

Run the **bgp shutdown** command to actively shut down all connections.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All connections of BGP are not shut down actively by default.

Syntax

bgp shutdown [**graceful** [**community** *community-value*] [**delay** *delay-time*]]

no bgp shutdown

default bgp shutdown

Parameter Description

graceful: Shuts down BGP connections in smooth manner.

community *community-value*: Specifies the community attribute value in a route sent to neighbors, in the format of AA:NN (AS number: 2-byte number) or a numeric. The value range is from 0 to 4294967295. If this parameter is not specified, the community attribute value is not carried.

delay *delay-time*: Specifies the delay time in seconds for shutting down BGP connections. The value range is from 1 to 65535. If this parameter is not specified, BGP connections are shut down on time.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to shut down valid BGP connections and delete all related routing information. If this command is configured in BGP configuration mode or scope configuration mode of BGP, all BGP connections are disabled in global configuration mode. If this command is configured in the configuration mode of the IPv4 VRF address family or the IPv6 VRF address family of BGP, all BGP connections in the corresponding VRF instances are shut down.

If BGP connections are shut down in smooth manner, the device sends a route carrying the LOCAL_PREF or MED attribute to its neighbors. Upon receiving the route update information, the neighbors adjust the service traffic route to bypass this device. After a period (this period is automatically calculated based on the number of advertised routes or it is specified), the device actively shuts down BGP connections with neighbors.

Examples

The following example shuts down all the BGP connections in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp shutdown
```

The following example shuts down all the BGP connections in global configuration mode in smooth manner.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp shutdown graceful
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 bgp sourced-paths

Function

Run the **bgp sourced-paths** command to import routes with multiple paths or multiple next hops from other protocol modules.

Run the **no** form of this command to import routes with single path or single next hop from other protocol modules.

Run the **default** form of this command to restore the default configuration.

BGP imports routes with single path or single next hop by default from other protocol modules.

Syntax

bgp sourced-paths *protocol-type* **all**

no bgp sourced-paths *protocol-type* **all**

default bgp sourced-paths *protocol-type* **all**

Parameter Description

protocol-type: Source protocol type of a redistributed route.

- **arp-host**: Specifies a host route converted from ARP.
- **isis**: Specifies an IS-IS route.

- **ospf**: Specifies an OSPF route.
- **rip**: Specifies an RIP route.
- **static**: Specifies a static route.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command needs to be used with the **redistribute** command to import routes with multiple next hops from other protocols to BGP.

Examples

The following example imports static routes with multiple paths or multiple next hops.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp sourced-paths static all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **redistribute**

1.64 bgp tcp-source-check disable

Function

Run the **bgp tcp-source-check disable** command to disable the function of TCP source address checking of BGP.

Run the **no** form of this command to enable this function.

Run the **default** form of this command to restore the default configuration.

The function of TCP source address checking is enabled by default.

Syntax

bgp tcp-source-check disable

no bgp tcp-source-check disable

default bgp tcp-source-check disable

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

After the function of TCP source address checking is disabled, BGP receives all TCP connection requests. After a TCP connection is established, a notification packet is sent to reject this connection if the local device is not configured with peers.

Examples

The following example disables the function of TCP source address checking of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp tcp-source-check disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.65 bgp timer accuracy-control

Function

Run the **bgp timer accuracy-control** command to enable the strict execution function of internal timers of BGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The strict execution function of internal timers of BGP is disabled by default.

Syntax

bgp timer accuracy-control

no bgp timer accuracy-control

default bgp timer accuracy-control

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

Internal timers of BGP can generate a random offset at a specified time by default. Therefore, you try not to allow excessive timers to time out concurrently. You can configure this command to allow BGP timers to strictly execute their functions according to the specified time. Unless in a special requirement, you are advised not to enable this function.

Examples

The following example enables the strict execution function of internal timers of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# bgp timer accuracy-control
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 bgp upgrade-cli

Function

Run the **bgp upgrade-cli** command to configure the CLI display mode of BGP as address family configuration mode or scope configuration mode.

Run the **no** form of this command to configure the CLI display mode of BGP as automatic identification based on user configuration.

Run the **default** form of this command to restore the default configuration.

The CLI display mode of BGP is configured as address family configuration mode by default.

Syntax

bgp upgrade-cli vrf { **af-mode** | **scope-mode** }

no bgp upgrade-cli vrf { **af-mode** | **scope-mode** }

default bgp upgrade-cli vrf { **af-mode** | **scope-mode** }

Parameter Description

af-mode: Configures the CLI display mode of BGP as address family configuration mode.

scope-mode: Configures the CLI display mode of BGP as scope configuration mode.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

You can run this command to switch the CLI display mode of BGP. The CLI display modes of BGP include address family configuration mode and scope configuration mode.

- If the CLI display mode is configured as address family configuration mode, all CLI commands are displayed in address family configuration mode.
- If the CLI display mode is configured as scope configuration mode, all CLI commands are displayed in scope configuration mode or address family configuration mode of the scope.

Examples

The following example configures the CLI display mode of BGP as scope configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 500
Hostname(config-router)# bgp upgrade-cli scope-mode
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.67 bmp server

Function

Run the **bmp server** command to configure a BMP server instance and enter the BMP configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BMP server instance is configured by default.

Syntax

bmp server *bmp-server-number*

no bmp server *bmp-server-number*

default bmp server *bmp-server-number*

Parameter Description

bmp-server-number: Number of a configured BMP server instance. The value range is from 1 to 8.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures BMP server instance 1 and enters the BMP configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 buffer-size

Function

Run the **buffer-size** command to configure the maximum number of packets or bytes in the buffer of a BMP instance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The number of packets or bytes in the buffer of a BMP instance is not limited by default.

Syntax

buffer-size *buffer-size-maximum*

no buffer-size

default buffer-size

Parameter Description

buffer-size-maximum: Maximum number of packets or bytes in the buffer of a BMP instance, in bytes. The value range is from 40960 to 4294967295.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

When a server cannot receive BMP packets due to insufficient memory or other reasons, the monitor packets on the server cannot be sent out and occupy the memory space. Therefore, you must limit the maximum number of packets or bytes in the buffer. When the number of packets or bytes in the buffer reaches the limit, the session with the BMP server is reset to release the cached packets.

Examples

The following example sets the maximum number of packets or bytes in the buffer of BMP instance 1 to **409600000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# buffer-size 409600000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.69 clear bgp advertise lowest-priority on-startup

Function

Run the **clear bgp advertise lowest-priority on-startup** command to restore the priority of advertised routes to BGP neighbors to the level before the configuration of the **bgp advertise lowest-priority on-startup** command**.**

Syntax

clear bgp advertise lowest-priority on-startup

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **bgp advertise lowest-priority on-startup** command is configured for a device, the device adjusts the priority of advertised routes to the lowest level after restart. You can run the **clear bgp advertise lowest-priority on-startup** command to restore the priority of advertised routes to the level before such adjustment.

Examples

The following example restores the route priority to the level before adjustment.

```
Hostname> enable
Hostname# clear bgp advertise lowest-priority on-startup
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.70 clear bgp all

Function

Run the **clear bgp all** command to clear all the address families of BGP.

Syntax

clear bgp all [*as-number*] [**soft**] [**in** | **out**]

Parameter Description

as-number: Specified AS in which the sessions of all peers are reset. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to reset the sessions of all supported address families, including sessions in the VRF instances of each address family. If the **soft** and **in** or **out** keywords are not specified, this command directly resets BGP sessions.

Examples

The following example clears all the address families of BGP.

```
Hostname> enable
Hostname# clear bgp all
```

Notifications

N/A

Platform Description

N/A

1.71 clear bgp all peer-group

Function

Run the **clear bgp all peer-group** command to clear a specified peer group of BGP.

Syntax

clear bgp all peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

peer-group-name: Specified peer group to be reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to reset the sessions of all supported address families, including session connections in the VRF instances of each address family. If no optional parameter is specified, this command directly resets BGP sessions.

Examples

The following example clears all the connections of all BGP peers in the peer group **test**.

```
Hostname> enable
Hostname# clear bgp all peer-group test
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.72 clear bgp all update-group

Function

Run the **clear bgp all update-group** command to clear the sessions of all members in an update group.

Syntax

clear bgp all update-group [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**soft**] [**in** | **out**]

Parameter Description

neighbor-ipv4-address: IPv4 address of the specified neighbor to be reset.

neighbor-ipv6-address: IPv6 address of the specified neighbor to be reset.

update-group-index: Index of a specified update group to be reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to reset the BGP sessions of all members in the update group. If the **soft** and **in** or **out** keywords are not specified, this command directly resets BGP sessions.

Examples

The following example clears the routing information received by all peers of all update groups that the neighbor 1.1.1.1 belongs to.

```
Hostname> enable
Hostname# clear bgp all update-group 1.1.1.1 in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.73 clear bgp ipv4 unicast

Function

Run the **clear bgp ipv4 unicast** command to clear the specified sessions of an IPv4 unicast address family.

Syntax

clear bgp ipv4 unicast [**vrf** vrf-name] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**]

Parameter Description

vrf-name: Specified VRF name. If this parameter is not specified, global VRF instances are specified.

*****: Resets all the peer sessions in the address family.

as-number: Specified AS in which all member sessions are reset. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

neighbor-ipv4-address: IPv4 address of the specified peer whose BGP sessions are reset.

neighbor-ipv6-address: IPv6 address of the specified peer whose BGP sessions are reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, this command directly resets BGP sessions.

Examples

The following example clears all sessions of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.74 clear bgp ipv4 unicast dampening

Function

Run the **clear bgp ipv4 unicast dampening** command to clear the route flapping information of an IPv4 unicast address family and remove route dampening.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **dampening** [*ipv4-address* [*mask*]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all route flapping information is cleared.

ipv4-address: IPv4 route address. If this parameter is not specified, the route flapping information and route dampening of all IPv4 addresses is cleared.

mask: Mask. If this parameter is not specified, the route flapping information and route dampening of a specified IPv4 address is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear the route flapping information of BGP to remove route dampening.

Examples

The following example clears the route flapping of the IPv4 unicast address family 192.168.0.0/16 and removes route dampening.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast dampening 192.168.0.0 255.255.0.0
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.75 clear bgp ipv4 unicast external

Function

Run the **clear bgp ipv4 unicast external** command to clear the EBGP connections of all IPv4 unicast address families.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **external** [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets routes received by all EBGP neighbors of an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast external in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.76 clear bgp ipv4 unicast flap-statistics

Function

Run the **clear bgp ipv4 unicast flap-statistics** command to clear the statistics about route flapping of an IPv4 unicast address family.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **flap-statistics** [ipv4-*address* [*mask*]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

ipv4-address: IPv4 route address. If this parameter is not specified, the statistics about route flapping of all IPv4 addresses is cleared.

mask: Mask. If this parameter is not specified, the statistics about route flapping of a specified IPv4 address is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to only clear the statistics about routes that are not dampened, but is not used to release dampened routes. To clear the statistics about all routes and release dampened routes, you can run the **clear ip bgp dampening** command.

Examples

The following example clears the statistics about route flapping of all IPv4 unicast address families.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast flap-statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.77 clear bgp ipv4 unicast peer-group

Function

Run the **clear bgp ipv4 unicast peer-group** command to clear the sessions of all members of a peer group in an IPv4 unicast address family.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **peer-group** *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

peer-group-name: Name of a peer group.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets routing information received by all peers of the peer group my-group in an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast peer-group my-group in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.78 clear bgp ipv4 unicast table-map

Function

Run the **clear bgp ipv4 unicast table-map** command to clear and update the Table-map configuration of an IPv4 unicast address family of BGP.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **table-map**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The Table-map configuration is reapplied to update the delivered core routing table.

Examples

The following example clears and updates the Table-map configuration of an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast table-map
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.79 clear bgp ipv4 unicast update-group

Function

Run the **clear bgp ipv4 unicast update-group** command to clear the sessions of all members of an update group in an IPv4 unicast address family.

Syntax

clear bgp ipv4 unicast [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor to be reset in the update group.

neighbor-ipv6-address: IPv6 address of a specified neighbor to be reset in the update group.

update-group-index: Index of a specified update group to be reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets the routing information received by all peers in the update group that the local device configured in the IPv4 unicast address family 1.1.1.1 belongs to.

```
Hostname> enable
Hostname# clear bgp ipv4 unicast update-group 1.1.1.1 in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.80 clear bgp ipv6 unicast

Function

Run the **clear bgp ipv6 unicast** command to clear the specified sessions of an IPv6 unicast address family of BGP.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

*****: Resets all the peer sessions in the address family.

as-number: Specified AS in which the sessions of all members are reset. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

neighbor-ipv4-address: IPv4 address of the specified peer whose BGP sessions are reset.

neighbor-ipv6-address: IPv6 address of the specified peer whose BGP sessions are reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example clears all the sessions of an IPv6 unicast address family of BGP.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.81 clear bgp ipv6 unicast dampening

Function

Run the **clear bgp ipv6 unicast dampening** command to clear the route flapping information and route dampening of an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **dampening** [*ipv6-address/prefix-length*]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all route flapping information is cleared.

ipv6-address/prefix-length: IPv6 route address and its prefix. If this parameter is not specified, the route flapping information and route dampening of all IPv6 addresses is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear the route flapping information of BGP to remove route dampening.

Examples

The following example clears the route flapping and dampening state of the IPv6 unicast address family 1::1/96.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast dampening 1::1/96
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.82 clear bgp ipv6 unicast external

Function

Run the **clear bgp ipv6 unicast external** command to clear all the EBGP connections of an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **external** [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets all the EBGP routes received by all EBGP neighbors of an IPv6 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast external in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.83 clear bgp ipv6 unicast flap-statistics

Function

Run the **clear bgp ipv6 unicast flap-statistics** command to clear the statistics about route flapping of an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **flap-statistics** [*ipv6-address/prefix-length*]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

ipv6-address/prefix-length: IPv6 route address and its prefix. If this parameter is not specified, the statistics about route flapping of all IPv6 addresses is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to only clear the statistics about routes that are not dampened, but is not used to release dampened routes. To clear the statistics about all routes and release dampened routes, you can run the **clear bgp ipv4 unicast dampening** command.

Examples

The following example clears the statistics about route flapping of all IPv6 unicast address families.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast flap-statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.84 clear bgp ipv6 unicast peer-group

Function

Run the **clear bgp ipv6 unicast peer-group** command to clear the sessions of all members of a peer group in an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **peer-group** *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

peer-group-name: Name of a peer group.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets the routing information received by all peers of the peer group my-group in an IPv6 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast peer-group my-group in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.85 clear bgp ipv6 unicast table-map

Function

Run the **clear bgp ipv6 unicast table-map** command to clear and update the Table-map configuration of an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **table-map**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, global VRF instances are specified.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears and updates the Table-map configuration of an IPv6 unicast address family.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast table-map
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.86 clear bgp ipv6 unicast update-group

Function

Run the **clear bgp ipv6 unicast update-group** command to clear all the member sessions of an update group in an IPv6 unicast address family.

Syntax

clear bgp ipv6 unicast [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-addres* | *update-group-index*] [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a Virtual Routing Forwarding (VRF) name. If this parameter is not specified, global VRF instances are specified.

neighbor-ipv4-address: IPv4 address of the specified neighbor to be reset in the update group.

neighbor-ipv6-address: IPv6 address of the specified neighbor to be reset in the update group.

update-group-index: Index of the specified update group to be reset.

soft: Performs a soft reset on routing information.

in: Resets received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft** and **in** or **out** keywords are not specified, BGP sessions are directly reset.

Examples

The following example resets the routing information received by all peers of the update group that the IPv6 unicast address family neighbor 1.1.1.1 belongs to.

```
Hostname> enable
Hostname# clear bgp ipv6 unicast update-group 1.1.1.1 in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.87 clear bmp

Function

Run the **clear bmp** command to reset BMP.

Syntax

clear bmp { **all** | **server** *server-number* }

Parameter Description

all: Resets all BMP servers.

server *server-number*: Resets the BMP server of a specified instance number. The value range is from 1 to 8.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to terminate and reconnect sessions with a BMP server.

Examples

The following example resets BMP.

```
Hostname> enable
Hostname# clear bmp all
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.88 clear ip bgp

Function

Run the **clear ip bgp** command to clear the specified sessions of an IPv4 unicast address family of BGP.

Syntax

clear ip bgp [**vrf** *vrf-name*] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

*****: Resets all peer sessions in the address family.

as-number: Specified AS in which the BGP sessions of all members are reset. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

neighbor-ipv4-address: IPv4 address of a specified peer whose BGP sessions are reset.

neighbor-ipv6-address: IPv6 address of a specified peer whose BGP sessions are reset.

soft: Performs a soft reset on routing information.

in: Reset received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft**, **in** or **out** parameter is not specified, BGP sessions are directly reset.

When a routing policy or BGP configuration changes, you can terminate and reestablish a BGP connection to execute the new routing policy or configuration. By configuring soft reset of BGP, you can execute a new routing policy without terminating a BGP session connection.

This command requires all connected BGP neighbors to support the routing update function. You can run the **show ip bgp neighbors** command to determine whether BGP peers support this function. If the BGP peers do not support this function, you can run the **neighbor soft-reconfiguration inbound** command to save original routing information for each specified BGP peer on the local BGP speaker. Saving routing information consumes device resources.

Examples

The following example resets sessions of all peers in an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# clear ip bgp *
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.89 clear ip bgp dampening

Function

Run the **clear ip bgp dampening** command to clear the route flapping information and route dampening of an IPv4 unicast address family.

Syntax

clear ip bgp [**vrf** *vrf-name*] **dampening** [*ipv4-address* [*mask*]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all route flapping information is cleared.

If the optional parameter is not carried, all route flapping information is cleared.

ipv4-address: IPv4 address. If this parameter is not specified, the route flapping information and route dampening of all IPv4 addresses is cleared.

mask: Mask. If this parameter is not specified, the route flapping information and route dampening of a specified IPv4 address is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear the route flapping information of BGP to remove route dampening.

Examples

The following example clears the flapping and dampening state of routes of the IPv4 unicast address family 192.168.0.0/16.

```
Hostname> enable
Hostname# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.90 clear ip bgp external

Function

Run the **clear ip bgp external** command to clear EBGP connections of all IPv4 unicast address families.

Syntax

clear ip bgp [**vrf** *vrf-name*] **external** [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

soft: Performs a soft reset on routing information.

in: Reset received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft**, **in** or **out** parameter is not specified, BGP sessions are directly reset.

Examples

The following example resets routes received by all EBGP neighbors of an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear ip bgp external in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.91 clear ip bgp flap-statistics

Function

Run the **clear ip bgp flap-statistics** command to clear statistics about route flapping of an IPv4 unicast address family.

Syntax

clear ip bgp [**vrf** *vrf-name*] **flap-statistics** [*ipv4-address* [*mask*]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

address: IPv4 address. If this parameter is not specified, the statistics about route flapping of all IPv4 addresses is cleared.

mask: Mask. If this parameter is not specified, the statistics about route flapping of a specified IPv4 address is cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to only clear statistics about routes that are not dampened but is not used to release dampened routes. To clear statistics about all routes and release dampened routes, you can run the **clear ip bgp dampening** command.

Examples

The following example clears statistics about route flapping of all IPv4 unicast address families.

```
Hostname> enable
Hostname# clear ip bgp flap-statistics
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.92 clear ip bgp peer-group

Function

Run the **clear ip bgp peer-group** command to clear sessions of all members in a peer group in an IPv4 unicast address family.

Syntax

clear ip bgp [**vrf** *vrf-name*] **peer-group** *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

peer-group-name: Name of a peer group.

soft: Performs a soft reset on routing information.

in: Reset received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft**, **in** or **out** parameter is not specified, BGP sessions are directly reset.

Examples

The following example resets routing information received by all peers of the peer group my-group in an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear ip bgp peer-group my-group in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.93 clear ip bgp table-map

Function

Run the **clear ip bgp table-map** command to clear old information and update the Table-map's routing information in an IPv4 unicast address family.

Syntax

clear ip bgp [**vrf** *vrf-name*] **table-map**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example updates the Table-map's routing information in an IPv4 unicast address family.

```
Hostname> enable
Hostname# clear ip bgp table-map
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.94 clear ip bgp update-group

Function

Run the **clear ip bgp update-group** command to clear sessions of all members in a peer group in an IPv4 unicast address family.

Syntax

clear ip bgp [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**soft**]] [**in** | **out**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor to be reset in the update group.

neighbor-ipv6-address: IPv6 address of a specified neighbor to be reset in the update group.

update-group-index: Index of a specified update group to be reset.

soft: Performs a soft reset on routing information.

in: Reset received routing information.

out: Resets distributed routing information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the **soft**, **in** or **out** parameter is not specified, BGP sessions are directly reset.

Examples

The following example resets the routing information received by all peers in the update group that the local device configured in the IPv4 unicast address family 1.1.1.1 belongs to.

```
Hostname> enable
Hostname# clear ip bgp update-group 1.1.1.1 in
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.95 default-information originate

Function

Run the **default-information originate** command to configure BGP to advertise redistributed default routes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BGP does not advertise redistributed default routes by default.

Syntax

default-information originate

no default-information originate

default default-information originate

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command and the **redistribute** command must be configured at the same time. This command takes effect only when the redistributed routes contain default routes.

This command is similar to the **network** command. When you configure the **default-information originate** command, you must run the **redistribute** command to redistribute default routes so as to validate such default routes. To configure the **network** command, you need to only configure default routes for Interior Gateway Protocol (IGP).

Examples

The following example configures BGP to advertise redistributed default routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# default-information originate
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.96 default-metric

Function

Run the **default-metric** command to use the manually configured metric value for a redistributed route of BGP.

Run the **no** form of this command to use the default metric value for a redistributed route of BGP.

Run the **default** form of this command to restore the default configuration.

The default metric value is used for a redistributed route of BGP.

Syntax

default-metric *metric-value*

no default-metric

default default-metric

Parameter Description

metric-value: Manually configured metric value. The value range is from 1 to 4294967295.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to configure the metric value for a redistributed route of BGP to ensure the complete metric value of the redistributed route.

The metric value configured by this command cannot overwrite the metric value configured by the **redistribute metric** command.

If this command is run for redistributed connected routes, the metric value is **0**.

Examples

The following example sets the default metric value of a BGP redistributed route to **45**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# default-metric 45
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.97 description

Function

Run the **description** command to configure description information of a BMP instance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No description information is configured for a BMP instance by default.

Syntax

description *description-text*

no description

default description

Parameter Description

description-text: Text describing this BMP instance. A maximum of 80 characters are entered.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

You can run this command to add description characters to a BMP instance so that users can mark the characteristics of this BMP instance.

Examples

The following example configures description information of a BMP instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# description test
```

Notifications

If over 80 characters are entered, the following notification will be displayed:

```
The description length exceed 80, please reconfig
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.98 distance bgp

Function

Run the **distance bgp** command to configure the administrative distance of a BGP route.

Run the **no** form of this command to restore the administrative distance of a BGP route to a default value.

Run the **default** form of this command to restore the default configuration.

The default administrative distance of a route learned by BGP from an EBGP peer is **20** and that of a route learned by BGP from an IBGP peer is **200**.

Syntax

distance bgp *external-distance internal-distance local-distance*

no distance bgp

default distance bgp

Parameter Description

external-distance: Administrative distance of routes learned from EBGP peers. The value range is from 1 to 255.

internal-distance: Administrative distance of routes learned from IBGP peers. The value range is from 1 to 255.

local-distance: Administrative distance of routes learned from peers, including better routes that can be learned from IGP. Generally, these routes are indicated by the **network backdoor** command. The value range is from 1 to 255, and the default value is **200**.

Command Modes

BGP configuration mode

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You are not advised to change the administrative distance of BGP routes. If it needs change, follow the rules below when configuring this command:

- The *external-distance* must be smaller than that of other IGP routing protocols such as OSPF and RIP.
- The *internal-distance* and *local-distance* must be greater than that of other IGP routing protocols.

Examples

The following example configures the administrative distance of a BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# distance bgp 20 20 200
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.99 exit-address-family

Function

Run the **exit-address-family** command to exit the address family configuration mode of BGP.

Each address family is configured with an exit mode by default.

Syntax

exit-address-family

Parameter Description

N/A

Command Modes

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can run this command to exit from different address family configuration modes to the BGP configuration mode.

Examples

The following example exits the current address family configuration mode of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# address-family ipv4 unicast
Hostname(config-router-af)# exit-address-family
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.100 failure-retry-delay

Function

Run the **failure-retry-delay** command to configure the time to reestablish a connection with a BMP server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The time to reestablish a connection with a BMP server is not configured by default.

Syntax

failure-retry-delay *retry-delay-interval*

no failure-retry-delay

default failure-retry-delay

Parameter Description

retry-delay-interval: Interval in seconds to reestablish a connection with a BMP server. The value range is from 30 to 720.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the time to reestablish a connection with a BMP server to **60** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# failure-retry-delay 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.101 import path selection

Function

Run the **import path selection** command to configure a route import policy.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Only preferred routes are imported by default.

Syntax

import path selection { **all** | **bestpath** | **multipath** }

no import path selection

default import path selection

Parameter Description

all: Imports all routes with next hops.

bestpath: Imports preferred routes with next hops.

multipath: Imports preferred and equivalent routes with next hops.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can use this command to import routing entries between different VRF instances.

Examples

The following example imports all routes with next hops to a global IPv4 routing table.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65530
Hostname(config-router)# import path selection all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.102 maximum-paths

Function

Run the **maximum-paths** command to configure EBGP/IBGP multipath load balancing and specify the number of equivalent paths.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

EBGP/IBGP multipath load balancing is not configured by default.

Syntax

maximum-paths { **ebgp** | **ibgp** } *maximum-paths-number*

no maximum-paths { **ebgp** | **ibgp** }

default maximum-paths { **ebgp** | **ibgp** }

Parameter Description

ebgp: Configures the number of equivalent paths of the EBGP multipath load balancing function.

ibgp: Configures the number of equivalent paths of the IBGP multipath load balancing function.

maximum-paths-number: Maximum number of equivalent paths. The value range is from 1 to 32. If the value is **1**, the function of EBGP multipath load balancing is disabled.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

If you specify the **ebgp** keyword when configuring this command, you can configure the function of multipath load balancing for routes of alliance EBGP and local VRF instances and specify the number of equivalent routes.

Note

This command does not allow IBGP and EBGP routes to form equivalent routes.

Examples

The following example configures EBGP load balancing and sets the maximum number of equivalent paths to **2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65530
Hostname(config-router)# maximum-paths ebgp 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.103 maximum-prefix

Function

Run the **maximum-prefix** command to configure the maximum number of route prefixes in a routing information base under an address family.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The number of route prefixes in a BGP routing information base under an address family is not limited by default.

Syntax

maximum-prefix *maximum-prefix-number*

no maximum-prefix

default maximum-prefix

Parameter Description

maximum-prefix-number: Maximum number of route prefixes in a BGP routing information base under an address family. The value range is from 1 to 4294967295.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The route prefixes of a BGP address family may be configured by the **redistribute** command, learned from neighbors, or imported from other VRF instances. When the number of route prefixes of this BGP address family reaches the threshold, the route prefixes of this address family do not increase. In this case, the table of this address family and all neighbors in this address family enter the overflow state. To clear this state, you must reconfigure BGP or run the **clear bgp** *addressfamily* ***** command to reset the address family.

You can run the **show bgp** { *addressfamily* | **all** } **summary** command to display the state of the routing information base.

Note

If an address family enters the overflow state because the number of BGP route prefixes reaches the threshold, you can configure the **maximum-prefix** parameter to change the state of the address family.

For IPv4 unicast routes, even if the address family reaches the overflow state, it can still receive route prefixes in the following scenarios:

- The routing information with same route prefixes is configured in the routing information base.
- The prefix of a route (except for the default route) is configured in the routing information base and the next hop of this route differs from that of the newly received route.

Examples

The following example sets the maximum number of prefixes in a BGP routing information base under an IPv4 unicast address family to **65535**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv4
Hostname(config-router-af)# maximum-prefix 65535
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.104 neighbor activate

Function

Run the **neighbor activate** command to activate neighbors or peer groups in current address mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No neighbor or peer group is activated by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **activate**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **activate**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **activate**

Parameter Description

neighbor-ipv6-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After the **neighbor remote-as** command is configured in an IPv4 Unicast address family of BGP or BGP configuration mode for the specified peer, the system automatically configures the **neighbor activate** command for this peer. In other address family configuration modes, the **neighbor activate** command must be manually configured.

Examples

The following example activates the route interaction capability of the neighbor 10.0.0.1 in the configuration mode of the IPv4 address family.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router)# address-family ipv4
Hostname(config-router-af)# neighbor 10.0.0.1 activate
```

Notifications

If configuration is completed in the scope VRF mode and the IPv4 address family is not activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name inactive.
```

If configuration is completed in the scope VRF mode and the IPv4 VRF mode is first activated by a VRF instance, the following notification will be displayed:

```
% Address family ipv4 unicast of vrf vrf-name enabled.
```

If the IPv6 unicast routing capability is not activated in global configuration mode and the neighbor address family capability of the IPv6 address is not configured or the neighbor is not activated, the following notification will be displayed:

```
% Can't activate ipv6 neighbor, please use ipv6 unicast routing first!
```

If the IPv6 routing capability for a neighbor is activated in an address family that does not support IPv6 addresses, the following notification will be displayed:

```
% IPv6 neighbor not supported in the address-family
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.105 neighbor additional-paths

Function

Run the **neighbor additional-paths** command to enable the ADD-PATH function of the specified peer.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The ADD-PATH function is disabled by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **additional-paths** { **send** [**receive**] | **receive** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **additional-paths** { **send** [**receive**] | **receive** }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **additional-paths** { **send** [**receive**] | **receive** }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

send: Enables the ADD-PATH route sending capability on a device. Only when the ADD-PATH receiving capability is enabled on peers can the device advertise ADD-PATH routes.

receive: Enables the ADD-PATH route receiving capability on a device. Only when the ADD-PATH sending capability is enabled on peers can the local device receive ADD-PATH routes.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Default Level

14

Usage Guidelines

The local device can advertise ADD-PATH routes only when the ADD-PATH sending capability is enabled on the local device and the ADD-PATH receiving capability is enabled on peers.

This command is effective to IBGP neighbors only. After this command is configured, BGP neighbor relationship is reestablished.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example enables the ADD-PATH function for the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 additional-paths send
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bgp additional-paths select**

1.106 neighbor advertise additional-paths

Function

Run the **neighbor advertise additional-paths** command to advertise the specific type of alternative ADD-PATH routes to peers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A device does not advertise alternative ADD-PATH routes to peers by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertise additional-paths** { **all** | **best** *best-number* | **ecmp** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertise additional-paths**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertise additional-paths**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

all: Advertises "all" types of alternative ADD-PATH routes.

best *best-number*: Advertises the "best number" type of alternative ADD-PATH routes. The value of the best number is **2** or **3**.

ecmp: Advertises the "ecmp" type of alternative ADD-PATH routes.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Default Level

14

Usage Guidelines

You can select a specific type of ADD-PATH routes by configuring the **bgp additional-paths select** command. When the type of the selected alternative ADD-PATH routes is different from that of the ones to be advertised, the device does not advertise the alternative ADD-PATH routes, but only the optimal route.

The local device can advertise ADD-PATH routes only when the ADD-PATH sending capability is enabled on the local device and the ADD-PATH receiving capability is enabled on peers.

This command is effective to IBGP neighbors only.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example configures neighbor 10.0.0.1 to advertise the "best number" type of routes as alternative ADD-PATH routes if permitted.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 advertise additional-paths best 2
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

- **bgp additional-paths select**
- **neighbor additional-paths**

1.107 neighbor advertisement-interval

Function

Run the **neighbor advertisement-interval** command to configure the route update interval of BGP.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default route update interval of BGP is **0** seconds for IBGP connections and **30** seconds for EBGP connections.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertisement-interval** *advertisement-interval*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertisement-interval**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **advertisement-interval**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

advertisement-interval: Route update interval, in seconds. The value range is from 0 to 600.

Command Modes

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example sets the interval of sending BGP route updates to the peer 10.0.0.1 to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router)# neighbor 10.0.0.1 advertisement-interval 10
```

Notifications

If a specified peer is a member of a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.108 neighbor aigp

Function

Run the **neighbor aigp** command to enable the AIGP function of BGP neighbors.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The AIGP function of BGP neighbors is disabled by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **aigp** [**send med**]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **aigp**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **aigp**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

send med: Converts AIGP Metric values to MED values when routes are advertised to a specified neighbor.

Command Modes

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Default Level

14

Usage Guidelines

If this command is not configured for a specified neighbor, the device neither receives AIGP attributes of this neighbor nor sends routes carrying the AIGP attributes to this neighbor.

If the neighbor device does not support the AIGP function, you can specify the **send med** keyword to convert the AIGP value to the MED value.

If the 64-bit AIGP Metric value is greater than 4294967295, the 32-bit MED value is 4294967295 after conversion.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example creates a neighbor and enables the AIGP function for this neighbor in the configuration mode of the BGP IPv4 VRF address family.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 aigp
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.109 neighbor allowas-in

Function

Run the **neighbor allowas-in** command to allow the local device to receive update packets that carry the AS number of the local device.

Run the **no** form of this command not to receive update packets that carry the AS number of the local device.

Run the **default** form of this command to restore the default configuration.

No update packets that carry the AS number of the local device are allowed to be received by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **allowas-in** [*occurrence-number*]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **allowas-in**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **allowas-in**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

occurrence-number: Occurrence times of an AS number. The value range is from 1 to 10, and the default value is **3**.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured on a PE device in the Hub-Spoke network, the PE device can receive update packets that carry the AS number of the local device. The PE device is configured with two VRF instances. Here, one VRF instance is used to receive routing information of all PE devices and advertise the information to a CE device. The other VRF instance is used to receive routing information of the CE device and advertise the information to all PE devices.

When this command is configured, a specified peer can be an IBGP or EBGP peer.

Examples

The following example creates a neighbor 10.0.0.1 in IPv4 VRF configuration mode of BGP and allows the local device to receive update packets that carry the AS number of the local device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 allowas-in
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.110 neighbor as-loop-check out

Function

Run the **neighbor as-loop-check out** command to enable the loop detection function in the outbound direction of a BGP neighbor.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The loop detection function in the outbound direction of a BGP neighbor is disabled by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-loop-check out**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as**-**loop**-**check out**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as**-**loop**-**check out**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

When the loop detection function in the outbound direction of a BGP neighbor is enabled, a device filters routes that carry the AS number of this neighbor in the AS_PATH attribute when it advertises routes to this neighbor.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example creates a neighbor in IPv4 VRF configuration mode of BGP and enables the loop detection function in the outbound direction of this neighbor.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 as-loop-check out
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.111 neighbor as-origination-interval

Function

Run the **neighbor as-origination-interval** command to configure the interval of advertising the local initial BGP route to a specified peer.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default interval of advertising the local initial BGP route to a specified peer is **1** second.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-origination-interval** *seconds*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-origination-interval**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-origination-interval**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

as-origination-interval: Interval in seconds of advertising the local initial BGP route. The value range is from 1 to 65535.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example creates a neighbor in IPv4 VRF configuration mode of BGP and sets the interval of advertising the local initial BGP route to the neighbor to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 as-origination-interval 10
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.112 neighbor as-override

Function

Run the **neighbor as-override** command to configure a PE device to overwrite the AS number of a site.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No PE is configured to overwrite the AS number of a site by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-override**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as**-**override**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as**-**override**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

Normally, BGP does not receive any routing information that has the same AS number as the local AS number. You can run this command to overwrite the AS number so that BGP can receive any routing information that is sent from the same AS number.

In a VPN, if two CE devices share the same AS number, they cannot receive peer information each other. After this command is configured on a PE device, the PE device overwrites the AS number of the CE devices so that they can receive routing information each other.

This command applies to only the specified EBGP peers.

Examples

The following example creates a neighbor in the configuration mode of the IPv4 VRF address family of BGP and overwrites the AS number of this neighbor site.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 as-override
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.113 neighbor bmp-active

Function

Run the **neighbor bmp-active** command to configure a specified BMP server to monitor neighbors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No neighbor is monitored by any BMP server by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **bmp-active** { **all** | **server** *server-number*&<1-8> }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **bmp**-**active** { **all** | **server** *server-number*&<1-8> }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **bmp**-**active** { **all** | **server** *server-number*&<1-8> }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

all: Specifies all BMP servers.

server-number&<1-8>: Instance number of a specified BMP server. The value range is from 1 to 8. &<1-8> specifies that the instance numbers of 1 to 8 specified BMP servers can be entered.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If you do not configure this command, no neighbor is monitored by any BMP server.

Examples

This command creates a neighbor in BGP configuration mode and specifies this neighbor to be monitored by all BMP servers.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router)# neighbor 10.0.0.1 bmp-active all
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.114 neighbor default-fast-withdraw

Function

Run the **neighbor default-fast-withdraw** command to allow a BGP speaker to quickly withdraw the default route from a peer (group).

Run the **no** form of this command to disable a BGP speaker from quickly withdrawing the default route from a peer (group).

Run the **default** form of this command to restore the default configuration.

No BGP speaker quickly withdraws the default route from a peer (group) by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-fast-withdraw**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-fast-withdraw**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-fast-withdraw**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, a device advertises a default route withdrawal message to this neighbor and then reselects a route if the original preferred route or equivalent route is not configured or is invalid.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example allows a BGP speaker to send a default route withdraw message to the peer 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.1.1.1 remote-as 80
Hostname(config-router)# neighbor 10.1.1.1 default-fast-withdraw
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.115 neighbor default-originate

Function

Run the **neighbor default-originate** command to allow a BGP speaker to advertise the default route to a peer (group).

Run the **no** form of this command to disable a BGP speaker from advertising the default route to a peer (group).

Run the **default** form of this command to restore the default configuration.

No BGP speaker is allowed to advertise the default route to a peer (group) by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-tag*]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-tag*]

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-tag*]

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

route-map *map-tag*: Name of a route-map. The route-map-name does not exceed 32 characters.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command allows the routing table of the local device to have a default route. After this command is configured, the device sends a default route with the next hop being the local device to its neighbors.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example configures a BGP speaker to advertise the default route to the peer 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.1.1.1 remote-as 80
Hostname(config-router)# neighbor 10.1.1.1 default-originate
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.116 neighbor description

Function

Run the **neighbor description** command to configure the description statement of a specified peer (group).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No description statement is configured for a specified peer (group) by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **description** *text*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **description**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **description**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

text: Text that describes this peer (group). A maximum of 80 characters are entered.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the description statement of the peer 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.1.1.1 remote-as 80
Hostname(config-router)# neighbor 10.1.1.1 description xyz.com
```

Notifications

If over 80 characters are entered, the following notification will be displayed:

```
The description length exceed 80, please reconfig
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.117 neighbor distribute-list

Function

Run the **neighbor distribute-list** command to implement an ACL-based routing policy when routing information is sent to and received from a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ACL-based routing policy is implemented by default when routing information is sent to and received from a specified BGP peer.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **distribute-list** { *access-list-name* | *access-list-number* } { **in** | **out** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **distribute-list** { *access-list-name* | *access-list-number* } { **in** | **out** }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **distribute-list** { *access-list-name* | *access-list-number* } { **in** | **out** }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

access-list-name: ACL name.

access-list-number: Number of an ACL. The value range is from 1 to 199 or from 1300 to 2699.

in: Applies the ACL to received routing information.

out: Applies the ACL to distributed routing information.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is configured based on address families. You can configure different filtering policies in different address families to control routing.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example filters the routes received from the peer 10.1.1.1 according to an ACL named **in**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.1.1.1 remote-as 80
Hostname(config-router)# neighbor 10.1.1.1 distribute-list bgp-filter in
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If an outbound policy is configured for the members in the peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If a prefix filtering list is configured for this peer (group), the following notification will be displayed:

```
% Prefix/distribute list can not co-exist, update the prefix/distribute list config
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.118 neighbor dmzlink-bw

Function

Run the **neighbor dmzlink-bw** command to carry the link bandwidth attribute in the specified neighbor's routes sent to IBGP neighbors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No link bandwidth attribute is carried in the specified neighbor's routes sent to IBGP neighbors by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **dmzlink-bw**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **dmzlink-bw**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **dmzlink-bw**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command applies to only EBGP neighbors with a specified single hop.

To send the extended community attribute of link bandwidth to IBGP neighbors, you must run the **neighbor send-community** command to enable the function of sending the extended community attribute.

Examples

The following example advertises to IBGP neighbors the extended community attribute of link bandwidth in IPv4 routes sent from an EBGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 dmzlink-bw
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **neighbor send-community**
- **show bgp all**

1.119 neighbor domain

Function

Run the **neighbor domain** command to configure a domain group for a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No domain group is configured for a specified BGP peer.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain** *domain-name*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

domain-name: Name of a domain group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

N/A

Examples

The following example classifies the peer 10.1.1.1 into the Domain test group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.1.1.1 remote-as 80
Hostname(config-router)# neighbor 10.1.1.1 domain test
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.120 neighbor domain-unsuppress

Function

Run the **neighbor domain-unsuppress** command to disable the domain group of a specified BGP peer from suppressing detailed routes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No domain group of a specified BGP peer is configured to suppress detailed routes.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain-unsuppress**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain**-**unsuppress**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **domain**-**unsuppress**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the domain group of the peer group test from suppressing detailed routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor test peer-group
Hostname(config-router)# neighbor test remote-as 80
Hostname(config-router)# neighbor test domain-unsuppress
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.121 neighbor ebgp-multihop

Function

Run the **neighbor ebgp-multihop** command to establish BGP connections with non-directly-connected EBGP peers.

Run the **no** form of this command not to establish BGP connections with non-directly-connected EBGP peers.

Run the **default** form of this command to restore the default configuration.

No BGP connections are established with non-directly-connected EBGP peers.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ebgp-multihop** [*ttl*]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ebgp**-**multihop**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ebgp**-**multihop**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

ttl: Maximum number of hops. The value range is from 1 to 255. If this parameter is not specified, the maximum number of hops is **255**.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

To avoid route loop and flapping, you must configure a route (except the default route) between the EBGP peers that are connected through multiple hops.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example establishes a BGP connection with the non-directly-connected EBGP peer 10.0.0.1 and sets the maximum number of hops to **255**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 ebgp-multihop 255
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.122 neighbor fall-over bfd

Function

Run the **neighbor fall-over bfd** command to correlate BGP with Bidirectional Forwarding Detection (BFD).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BGP is not correlated with BFD by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **fall-over bfd**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **fall-over bfd**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **fall-over bfd**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can run this command to detect changes of a specific neighbor and accelerate BGP convergence.

Before configuration, you must configure the BFD session parameters for the interface of the IP address of the neighbor.

Examples

The following example enables BGP correlation with BFD and uses Bidirectional Forwarding Detection (BFD) to detect the forwarding route to the neighbor 172.16.0.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 45000
Hostname(config-router)# neighbor 172.16.0.2 remote-as 45001
Hostname(config-router)# neighbor 172.16.0.2 fall-over bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.123 neighbor filter-list

Function

Run the **neighbor filter-list** command to apply the AS path filtering rule to the routing information received from and sent to a specified BGP peer (group).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No AS path filtering rule is applied to the routing information received from and sent to a specified AS peer (group) by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **filter-list** *as-path-access-list-number* { **in** | **out** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **filter-list** *as-path-access-list-number* { **in** | **out** }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **filter-list** *as-path-access-list-number* { **in** | **out** }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

neighbor filter-list: Number of the AS path filtering list. The value range is from 1 to 500.

in: Applies the AS path filtering list to received routing information.

out: Applies the AS path filtering list to distributed routing information.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is configured based on address families. You can configure different filtering policies in different address families to control routing.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example applies the AS path filtering list 1 to the routing information sent to the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip as-path access-list 1 deny _123_
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 filter-list 1 out
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If an outbound policy is configured for the members in the peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.124 neighbor global-nexthop-replace-local

Function

Run the **neighbor global-nexthop-replace-local** command to use the local address of a BGP IPv6 link as the global next hop address when IPv6 routing information is sent to the local peer (group) of the BGP IPv6 link.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The local address of a BGP IPv6 link is not used as the global next hop address by default when IPv6 routing information is sent to the local peer (group) of the BGP IPv6 link.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **global-nexthop-replace-local**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **global-nexthop-replace-local**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **global-nexthop-replace-local**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

By default, two next hop addresses, namely, the global address and local address, are carried in the IPv6 routing information that is sent to the local peer (group) of the BGP IPv6 link. If this command is configured for the peer (group), the global next hop address advertised to this peer (group) is replaced with the local address of the next hop link.

This command is not effective to the non-link local peer (group).

Examples

The following example uses the local address of a link as the global next hop address when a route is advertised to the peer FE80::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# neighbor FE80::1%vlan101 remote-as 1
Hostname(config-router-af)# neighbor FE80::1%vlan101 global-nexthop-replace-local
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.125 neighbor ha-mode nsr

Function

Run the **neighbor ha-mode nsr** command to enable the nonstop routing (NSR) function for a specified BGP peer (group).

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The NSR function for a BGP peer (group) is disabled by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ha-mode nsr**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ha-mode nsr**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ha-mode nsr**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

ha-mode: Specifies the high availability (HA) mode.

nsr: Enables the NSR mode.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The NSR function synchronizes state and data information between the active BGP and standby BGP of VSU. When the active BGP fails, the standby BGP can take over the BGP services to keep route availability.

A neighbor can enable multiple address families. The BGP NSR function is supported in only the IPv4/IPv6 Unicast address families. If a neighbor activates other address families, the NSR function cannot be enabled.

Examples

The following example enables the NSR function for the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 ha-mode nsr
```

Notifications

N/A

Common Errors

N/A

Platform Description

Related Commands

N/A

1.126 neighbor link state group

Function

Run the **neighbor link state group** command to associate a BGP peer (group) with a link state tracking group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BGP peer (group) is associated with any link state tracking group by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **link state group** *link-state-group-number*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **link state group**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **link state group**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

link-state-group-number: ID of a link state tracking group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

N/A

Examples

The following example associates the peer 10.0.0.1 with the link state tracking group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 link state group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.127 neighbor local-as

Function

Run the **neighbor local-as** command to configure the local AS number for a specified BGP peer (group).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local AS number is configured for a BGP peer (group) by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **local-as**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **local-as**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

as-number: Configured local AS number. The value range is from 1 to 65535. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

no-prepend: Does not add the local AS number to the AS-PATH attribute in the routing information received from a peer. If this parameter is not specified, the local AS number is added to the AS-PATH attribute in the routing information received from a peer.

replace-as: Replaces the BGP AS number with the local AS number in the AS-PATH attribute of the routing information sent to a peer. If this parameter is not specified, the BGP AS number is not replaced with the local AS number in the AS-PATH attribute of the routing information sent to a peer.

dual-as: Enables a peer to use the BGP AS number or local AS number to establish a BGP connection with a device. If this parameter is not specified, the peer can use only the local AS number to establish a BGP connection with the local device.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command applies to only the specified EBGP peers. If the attributes of the peers change, for example, the EBGP peers change to IBGP peers or alliance EBGP peers, the local AS number and options configured for

these peers are deleted. The configured local AS number must be different from the BGP AS number and the remote AS number of the peers. If an alliance is configured, the local AS number must differ from the alliance ID. If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. Users are not allowed to separately configure a local AS number for a member in the peer group.

After this command is configured, a peer device can use this local AS number as a remote AS number to establish a BGP connection with the local device. If you do not specify any optional item for this command, the peer device can use only the local AS number to establish a BGP connection with the local device. The peer device also adds the local AS number to the AS-PATH attribute of the received routing information before routing information is sent to the peer.

Examples

The following example sets the local AS number of the peer 10.0.0.1 to **23**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 65100
Hostname(config-router)# neighbor 10.0.0.1 local-as 23
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.128 neighbor maximum-prefix

Function

Run the **neighbor maximum-prefix** command to configure the maximum number of prefixes received from a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The number of prefixes received from a specified BGP peer is not limited by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **maximum-prefix** *maximum-prefix-value* [*maximum-prefixthreshold*] [**restart-time** *restart-time* | **warning-only** [**suppress**]]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **maximum**-**prefix**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **maximum**-**prefix**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

maximum-prefix-value: Maximum number of prefixes that can be received. The value range is from 1 to 4294967295.

maximum-prefix-threshold: Percentage of the prefix number that triggers an alarm to the maximum number of prefixes. The value range is from 1 to 100, and the default value is **75**.

restart-time: Specifies the time of restoring the state machine of the neighbor after the local device enters the idle state because the number of route prefixes exceeds the upper limit.

restart-time: Time of restoring the state machine of a specified neighbor. The value range is from 1 to 65535.

warning-only: Generates a log without terminating a BGP connection when the number of route entries reaches the upper limit.

suppress: Stops learning entries when the number of route entries reaches the upper limit.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

When the received routing information exceeds the configured upper limit, the device terminates the BGP connection by default. If the **warning-only** keyword is specified when this command is configured, the device can retain the BGP connection when the received routing information exceeds the configured upper limit.

If the **suppress** keyword is specified when this command is configured, the device can stop learning route entries when the received routing information exceeds the configured upper limit. In this case, real route entries exceed the configured upper limit of the device. Because the route learning sequence may change before and after the reestablishment of neighbor relationships, the learned entries may be inconsistent.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example sets the maximum number of IPv4 unicast routes that are received by the peer 10.0.0.1 to **1000**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 maximum-prefix 1000
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.129 neighbor next-hop-self

Function

Run the **neighbor next-hop-self** command to configure the next hop of a route advertised to a specified BGP peer as the local device.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The next hop of a route advertised to an EBGP peer is configured as the local BGP speaker, and the next hop of a route advertised to an IBGP peer is not changed by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next-hop-self**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next**-**hop**-**self**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next**-**hop**-**self**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used in non-full-mesh networks such as Frame Relay and X.25. In this type of networks, the BGP speakers in the same subnet may not access each other directly.

If you specify a BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example configures the next hop of an IPv4 unicast route advertised to the peer 10.0.0.1 as the local BGP speaker.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 next-hop-self
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If a peer (group) is configured with an unchanged next hop, the following notification will be displayed:

```
% Cannot co-exist with next-hop-unchanged, Deconfigure first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.130 neighbor next-hop-unchanged

Function

Run the **neighbor next-hop-unchanged** command to retain the next hop of a route advertised to a specified peer (group).

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The next hop of a route advertised to an EBGP peer is changed to the local BGP speaker, and the next hop of a route advertised to an IBGP peer is not changed.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next-hop-unchanged**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next-hop-unchanged**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **next-hop-unchanged**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

next-hop-unchanged: Retains the next hop of a route sent to a BGP peer (group).

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast address family of BGP

Configuration mode of the IPv6 unicast address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is not configured on a route reflector. If you configure this command on the client of a route reflector, you cannot run the **neighbor next-hop-self** command on the client to modify the next hop of the route.

Examples

The following example advertises an IPv4 route to the peer 10.1.1.1 without changing the next hop of the route.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# address-family ipv4
Hostname(config-router-af)# neighbor 10.1.1.1 next-hop-unchanged
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If a peer (group) is configured with a next hop being itself, the following notification will be displayed:

```
% Cannot co-exist with next-hop-self, Deconfigure first
```

If a peer (group) is not a multi-hop EBGP neighbor, the following notification will be displayed:

```
% Can propagate the nexthop only to multi-hop EBGP neighbor
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.131 neighbor password

Function

Run the **neighbor password** command to enable TCP MD5 authentication and configure a password when a BGP connection is established with a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

TCP MD5 authentication is not enabled by default when a BGP connection is established with a specified BGP peer.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **password** [**0** | **7**] *password-string*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **password**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **password**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

0: Displays an unencrypted password.

7: Displays an encrypted password.

password-string: Password used for TCP MD5 authentication. A maximum of 80 characters are entered.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command calls TCP MD5 authentication. Therefore, you must configure the same password for the peers that have established a BGP connection with the local device. Otherwise, the neighbor relationship cannot be established. After this command is configured, the local device reestablishes a BGP connection with the BGP peers.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

You can configure one password only for each neighbor. In any address family configuration mode or BGP configuration mode, the configured password for a specified neighbor overwrites the original one.

Examples

The following example sets the password for TCP MD5 authentication of the peer 10.0.0.1 to **test**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 password test
```

Notifications

If the configured plaintext password exceeds 80 characters, the following notification will be displayed:

```
% Password length too large, must be less or equal than 80
```

If the configured cyphertext password exceeds 162 characters, the following notification will be displayed:

```
% Password length too large, must be less or equal than 162
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.132 neighbor peer-group (assigning members)

Function

Run the **neighbor peer-group** command to configure a specified BGP peer as a member of a BGP peer group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No specified BGP peer is configured as a member of a BGP peer group.

Syntax

neighbor { neighbor-ipv4-address | neighbor-ipv6-address } **peer-group** *peer-group-name*

no neighbor { neighbor-ipv4-address | neighbor-ipv6-address } **peer-group** *peer-group-name*

default neighbor { neighbor-ipv4-address | neighbor-ipv6-address } **peer-group** *peer-group-name*

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

A member of a peer group can inherit all configurations of a peer.

You can separately configure commands for each member in the peer group to overwrite unified configuration of the peer group. The configured commands do not include those configurations that influence route update. Each member in the peer group inherits the following configurations of the peer group:
remote-as, **update-source**, **local-as**, **reconnect-interval**, **times**, **advertisemet-interval**, **default-originate**, **next-hop-self**, **remove-private-as**, **send-community**, **distribute-list out**, **filter-list out**, **prefix-list out**, **route-map-name out**, **unsuppress-map**, **route-reflector-client**, and **as-origination-interval**.

Note

You may not put neighbors in different address families into the same peer group, nor add IBGP peers and EBGP peers to the same peer group.

Examples

The following example adds the peer 10.0.0.1 to the peer group **test**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor test peer-group
Hostname(config-router)# neighbor 10.0.0.1 peer-group test
```

Notifications

If the configured neighbor has the same address as the local interface, the following notification will be displayed:

```
% Cannot configure the local system as neighbor
```

When the IPv6 unicast routing capability is not activated in global configuration mode, if an IPv6 neighbor is configured, the following notification will be displayed:

```
% Cannot configure IPv6 neighbor, please use ipv6 unicast-routing first!
```

If the peer group is not configured, the following notification will be displayed:

```
% Configure the peer-group first
```

If no Remote AS is configured for the peer group and members are created in the peer group, the following notification will be displayed:

```
% Specify remote-as or peer-group remote AS first
```

If a configured peer belongs to another peer group, the following notification will be displayed:

```
% Cannot change the peer-group. Deconfigure first
```

If a member in the peer group and a configured peer belong to different types, the following notification will be displayed:

```
% Peer with AS as-number cannot be in this peer-group, members must be all internal
or all external
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.133 neighbor peer-group (creating)

Function

Run the **neighbor peer-group** command to create a BGP peer group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The function of a BSP peer group is disabled by default.

Syntax

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer**-**group**

default neighbor *peer-group-name* **peer**-**group**

Parameter Description

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If BGP peers share the same distribution list, update source or route filtering policy, you can assign these peers to the same peer group to simplify configuration and improve calculation update efficiency.

Examples

The following example creates a peer group **test**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor test peer-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.134 neighbor pic-disable

Function

Run the **neighbor pic-disable** command to disable the private PIC processing on routes distributed to and received from specified BGP peers.

Run the **no** form of this command to enable the private PIC process for routes advertised to and received from BGP peers.

Run the **default** form of this command to restore the default configuration.

A device performs the private PIC processing on routes sent to and received from BGP peers by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **pic-disable**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **pic-disable**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **pic-disable**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The CF type and E1 subtype of extended community attributes are used as the extended community attributes of the private PIC processing. This command is configured to disable the private PIC processing to ensure the compatibility of the extended community attributes for device connection with products of other vendors.

Examples

The following example disables the private PIC processing for the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 pic-disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.135 neighbor prefix-list

Function

Run the **neighbor prefix-list** command to implement the prefix list-based routing policy for routing information sent to and received from the specified BGP peers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No prefix list-based routing policy is implemented for routing information sent to and received from the specified BGP peers by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **prefix-list** *prefix-list-name* { **in** | **out** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **prefix-list** *prefix-list-name* { **in** | **out** }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **prefix-list** *prefix-list-name* { **in** | **out** }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

prefix-list-name: Name of a prefix list. It contains not more than 32 characters.

in: Applies the prefix list to received routing information.

out: Applies the prefix list to distributed routing information.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is configured based on address families. You can configure different filtering policies in different address families to control routing.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example configures a prefix list bgp-filter to filter routes received from the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip prefix-list bgp-filter deny 10.0.0.1/16
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter in
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If an outbound policy is configured for the members in the peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.136 neighbor remote-as

Function

Run the **neighbor remote-as** command to configure a BGP peer (group).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BGP peer (group) is configured by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

as-number: AS number of a BGP peer (group). A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example creates an EBGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 80
```

Notifications

If the address of a BGP neighbor is a local IPv6 link address, the following notification will be displayed:

```
% Using IPv6 link-local address as peer address must specify update-source interface
```

Common Errors

The address of a BGP neighbor is a local address.

```
% Cannot configure the local system as neighbor
```

IGBP neighbors are configured in BGP IPv4 VRF or BGP IPv6 VRF configuration mode.

```
% PE - CE peering must be EBGP.
```

Platform Description

N/A

Related Commands

N/A

1.137 neighbor remove-private-as

Function

Run the **neighbor remove-private-as** command to remove the private AS number from the AS_PATH attribute of the routes sent to a specified EBGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The private AS number is not removed from the AS_PATH attribute of the routes sent to a specified EBGP peer by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remove-private-as** [**force** [**ignore-remote-as**]] [**replace-as**]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remove**-**private**-**as**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remove**-**private**-**as**

Parameter Description

neighbor-ipv4-address: IPv4 address of the specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

force: Forcibly removes the private AS number.

ignore-remote-as: Ignores the private AS number.

replace-as: Replaces the private AS number with the local AS number.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is effective to EBGP peers only.

The AS number range is from 1 to 4294967295. The range of private AS numbers is from 64512 to 65534 or from 4200000000 to 4294967294, and they are used for specific private applications. Normally, you can configure this command to prevent the private AS number from being leaked to a public network.

If the following conditions are met, the software does not remove the private AS number from the AS_PATH attribute of routes:

- The AS_PATH attribute contains both the private AS number and public AS number.
- The private AS number contained in the AS_PATH attribute will be sent to an EBGP peer to prevent route loop.

If the preceding two conditions are met, you can specify the **force** parameter to forcibly remove a private AS number.

When the private AS number is removed forcibly, you can specify the **force ignore-remote-as** parameter to ignore the neighbor AS number.

You can specify the **replace-as** parameter to replace the private AS number with the local AS number to prevent the AS path from being shortened and thus avoid selecting a wrong route.

Examples

The following example removes the private AS from the AS-PATH attribute of routes advertised to the EBGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
```

```
Hostname(config-router)# neighbor 10.0.0.1 remove-private-as
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If configuration is completed for an IBGP peer, the following notification will be displayed:

```
% Private AS cannot be removed for IBGP peers
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.138 neighbor route-map

Function

Run the **neighbor route-map** command to match a received or an advertised route with a route map.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no route map is configured to match a received or an advertised route.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

map-tag: Name of a route map.

in: Applies a route map to received routes.

out: Applies a route map to advertised routes.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command can apply different rules to filter routes received from or sent to different neighbors to purify and control routing.

This command is configured based on address families. You can configure different filtering policies in different address families.

Examples

The following example filters routes received from the peer 10.0.0.1 by using the route map map-tag.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 route-map map-tag in
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If an outbound policy is configured for the members in the peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.139 neighbor route-reflector-client

Function

Run the **neighbor route-reflector-client** command to configure the local device as a route reflector and specify a client for it.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The local device is not configured as a route reflector by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route-reflector-client**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route**-**reflector**-**client**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route**-**reflector**-**client**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of the specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

All IGBP speakers in an AS must establish a full mesh of neighbor relationships by default. To avoid route loop, a BGP speaker does not forward a learned IBGP route to other IGBP peers.

After this command is configured, all IGBP speakers in the AS do not need to establish a full mesh of neighbor relationships, and the route reflector forwards the learned IBGP route to the client of the route reflector.

Examples

The following example configures the peer 10.0.0.1 as the client of a route reflector.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 route-reflector-client
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If configuration is completed for an EBGP peer (group), the following notification will be displayed:

```
% Invalid command. Not an internal neighbor
```

If this capability is configured for a peer group and disabled for the members in the peer group, the following notification will be displayed:

```
% This peer is a peer-group member.  Please change peer-group configuration
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.140 neighbor send-community

Function

Run the **neighbor send-community** command to advertise community attributes to a specified BGP neighbor.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No community attribute is advertised to a specified BGP neighbor by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **send-community** [**both** | **standard** | **extended**]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **send-community** [**both** | **standard** | **extended**]

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **send-community** [**both** | **standard** | **extended**]

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

both: Transmits standard and extended community attributes.

both: Transmits only standard community attributes.

both: Transmits only extended community attributes.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can configure this command to transmit specified community attributes to a specified neighbor or a group of neighbors.

Examples

The following example carries the community attributes in the routes advertised to the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 send-community both
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If configuration is completed for an EBGP peer (group), the following notification will be displayed:

```
% Invalid command. Not an internal neighbor
```

If this capability is configured for a peer group and disabled for the members in the peer group, the following notification will be displayed:

```
% This peer is a peer-group member.  Please change peer-group configuration
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.141 neighbor shutdown

Function

Run the **neighbor shutdown** command to shut down the connection of a specified peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The function of a specified BGP peer is enabled by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **shutdown** [**graceful** [**community** *community-value*] [**delay** *delay-time*]]

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **shutdown**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **shutdown**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

graceful: Shuts down BGP connections in smooth manner.

community *community-value*: Specifies the community attribute value carried in a route sent to a neighbor. It follows the format of AA:NN (AS number: 2-byte number) or the value is a numeric. The value range is from 0 to 4294967295.

delay *delay-time*: Specifies the delay time for shutting down BGP connections. The value range is from 1 to 65535.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is used to shut down the valid connection established with a specified peer (group) and delete all related routing information. The software retains any configuration of this specified peer (group).

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

If a BGP connection is shut down in smooth manner, the device sends a route carrying the Community, LOCAL_PREF, or MED attribute to a specified neighbor. After the neighbor receives the route update information.

After a period (this period is automatically calculated based on the number of advertised routes or it is specified), the device actively shuts down BGP connections with neighbors.

Examples

The following example actively shuts down the connection with the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 shutdown
```

The following example shuts down the connection with the peer 10.0.0.1 in a smooth manner.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 60
Hostname(config-router)# neighbor 10.0.0.1 shutdown graceful
```

Notifications

If this function is enabled on a peer group and configuration of group members is deleted, the following notification will be displayed:

```
% Peer-group has been shutdown. Activate the peer-group first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.142 neighbor soft-reconfiguration inbound

Function

Run the **neighbor soft-reconfiguration inbound** command to save original routing information sent by a specified BGP peer.

Run the **no** form of this command not to save original routing information of a specified BGP peer.

Run the **default** form of this command to restore the default configuration.

No original routing information of a specified BGP peer is saved by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command causes a BGP session to restart and retains the unchanged routing information sent by a BGP peer (group).

Configuring this command consumes more memory. If the local device and BGP peer support the route update function, you do not need to configure this command. You can run the **show ip bgp neighbors** command to judge whether a BGP peer supports the route update function.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example retains the original routing information of the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 soft-reconfiguration inbound
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If this capability is configured for a peer group and disabled for the members in the peer group, the following notification will be displayed:

```
% This peer is a peer-group member.  Please change peer-group configuration
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.143 neighbor soo

Function

Run the **neighbor soo** command to configure the Site-of-Origin (SoO) attribute of a neighbor.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No neighbor is configured with the SoO attribute by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soo** *soo-value*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soo**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soo**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

soo-value: Value of the SoO attribute. *soo-value* can be set as follows:

- *soo-value=as-number*: *nn*

  as-number is a public 2-byte AS number. *nn* is user-defined in the range from 0 to 4294967295.

- *soo-value=ip-address*: *nn*

  ip-address must be a global IP address. *nn* is user-defined in the range from 0 to 65535.

- *soo-value=as4-number*: *nn*

  as4-number is a public 4-byte AS number. *nn* is user-defined in the range from 0 to 65535.

Command Modes

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

When multiple CE devices of a VPN site use a BGP protocol to be connected with different PE devices, VPN routes sent from the CE devices to the PE devices may go back to this site. This situation causes a route loop in the site.

After this command is configured, if a PE device receives a route from a CE device, the PE device adds the SoO attribute to the route before forwarding the route to other PE devices. The other PE devices check the SoO attribute before they advertise the route to the CE device. If this attribute is consistent with that configured locally, the PE devices do not advertise the route to the CE device.

Examples

The following example configures the SoO attribute for the peer 10.0.0.1 in a VRF instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family ipv4 vrf vpn1
Hostname(config-router-af)# neighbor 10.0.0.1 remote-as 100
Hostname(config-router-af)# neighbor 10.0.0.1 soo 100:100
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.144 neighbor timers

Function

Run the **neighbor timers** command to configure the duration of Keepalive, Hold-Time, and Connect-Retry timers that are used to establish a BGP connection with a specified BGP peer.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The Keepalive timer duration is **60** seconds, Hold-Time timer duration is **180** seconds, and Connect-Retry timer duration is **15** seconds by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **timers** { *keepalive-interval holdtime* [*minimum-holdtime*] | **connect** *connect-retry* }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **timers** [**connect**]

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **timers** [**connect**]

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

keepalive-interval: Interval in seconds to send Keepalive messages to a specified BGP peer. The value range is from 0 to 65535, and the default value is **60**.

holdtime: Valid interval in seconds of a BGP peer. The value range is from 0 to 65535, and the default value is **180**.

minimum-holdtime: Minimum hold time in seconds of an advertisement from a neighbor. The value range is from 0 to 65535, and the value **0** specifies no limit.

connect: Specifies the reconnection time.

connect-retry: Interval in seconds to initiate a reconnection to a specified BGP peer. The value range is from 1 to 65535, and the default value is **15**.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

The *keepalive-interval* value cannot be greater than 1/3 of the *holdtime*.

If time is configured for a single peer or peer group, this peer or peer group is connected with peers based on the configured time other than the globally configured time.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

If you remove this command or restore the default configuration and specify the **connect** parameter, the command takes effect to the reconnection time. If you do not specify the **connect** parameter, the command takes effect to the sending interval and hold time of Keepalive messages.

Examples

The following example configures the sending interval and hold time of Keepalive messages of the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 timers 80 240
```

The following example configures the reconnection time of the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
```

```
Hostname(config-router)# neighbor 10.0.0.1 timers connect 100
```

Notifications

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

If the configured hold time is smaller than 3 but not equal to 0, the following notification will be displayed:

```
% Hold time must be 0 or greater than 2 seconds
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.145 neighbor transport connection-mode

Function

Run the **neighbor transport connection-mode** command to configure the connection establishment mode of BGP neighbors.

Run the **no** form of this command to restore the connection establishment mode of BGP neighbors to a default value.

Run the **default** form of this command to restore the default configuration.

A BGP neighbor can actively or passively establish connections by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **transport connection-mode** { **active-only** | **both** | **passive-only** }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **transport connection-mode**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **transport connection-mode**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

active-only: Specifies a neighbor to only actively establish connections.

Both: Specifies a neighbor to actively or passively establish connections.

passive-only: Specifies a neighbor to only passively establish connections.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You cannot concurrently configure the **active-only** or **passive-only** parameter for two devices that work as peers mutually.

Neighbors in a network segment can passively establish connections only, and their connection modes are not controlled by this command.

Examples

The following example configures only active connections for the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 45000
Hostname(config-router)# neighbor 10.0.0.1 remote-as 45001
Hostname(config-router)# neighbor 10.0.0.1 transport connection-mode active-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.146 neighbor ttl-security hops

Function

Run the **neighbor ttl-security hops** command to configure GTSM security check for BGP neighbors.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of GTSM security check is not configured by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ttl-security hops** *hop-count*
no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ttl-security hops**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ttl-security hops**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

hop-count: Maximum number of hops from a specified local device to a specified peer. The value range is from 1 to 255.

Command Modes

BGP configuration mode

IPv4 VRF configuration mode of BGP

IPv6 VRF configuration mode of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, the packets from a specified peer can be passed if their TTL values are within the specified range. Otherwise, the packets are discarded.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example enables the function of GTSM security check for BGP packets of the peer 10.0.0.1 and sets the maximum number of hops from a specified peer to a local device to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 ttl-security hops 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.147 neighbor unsuppress-map

Function

Run the **neighbor unsuppress-map** command to selectively advertise the routing information that is suppressed by route aggregation.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Routing information suppressed by route aggregation is not selectively advertised by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **unsuppress-map** *map-tag*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **unsuppress**-**map** *map-tag*

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **unsuppress**-**map** *map-tag*

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

map-tag: Name of a route map. It contains not more than 32 characters.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command can advertise the specified suppressed routes.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If this command is configured for a member in the peer group, this command overwrites the peer group-based configuration.

Examples

The following example uses the route map unspress-route to filter routes advertised to the peer 10.0.0.1 and advertises the matched routing information suppressed by route aggregation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 unsuppress-map unspress-route
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

If configuration is completed for the members in a peer group, the following notification will be displayed:

```
% Invalid command for a peer-group member
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.148 neighbor update-delay

Function

Run the **neighbor update-delay** command to delay the advertisement of BGP peers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The advertisement of BGP peers is not delayed by default.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update-delay** *update-delay-time*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update**-**delay**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update**-**delay**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

update-delay-time: Delay time in seconds of first route advertisement of a specified BGP peer. The value range is from 0 to 3600, and the value **0** specifies no limit.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can configure this command to specify the delay time of route advertisement during the first establishment of a connection with the BGP peer 10.0.0.1.

After BGP is enabled, neighbors will negotiate to reach the established state and send update packets to each other. If you configure this command, the local device sends routes received from a specified neighbor to other neighbors after a specified delay time. If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command.

Examples

The following example sets the delay time of first route advertisement to **60** seconds during the first establishment of a connection with the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 update-delay 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.149 neighbor update-source

Function

Run the **neighbor update-source** command to configure a network interface used to establish a BGP connection with a specified IBGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The optimal local interface is used as the output interface by default.

Syntax

neighbor { *neighbor-ipv4-address* | *peer-group-name* } **update-source** { *interface-type interface-number* | *source-ipv4-address* }

neighbor { *neighbor-ipv6-address* | *peer-group-name* } **update-source** { *interface-type interface-number* | *source-ipv6-address* }

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update-source**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update-source**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

interface-type interface-number: Interface type and interface number.

source-ipv4-address: IPv4 address of the network interface used to establish a BGP connection.

source-ipv6-address: IPv6 address of the network interface used to establish a BGP connection.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

Note

You are advised to use this command to specify a source address if you establish multiple peer relationships between two devices through multiple links.

You can run this command to establish a BGP connection with BGP peers through the loopback interface.

If you directly specify a network interface to establish a BGP connection, the address of the network interface must be a local valid one. Otherwise, the BGP connection cannot be established.

If this command is configured for a specified BGP peer group, all members in the peer group inherit the configuration of this command. If a network interface is specified, a member in a peer group can inherit the configuration of this command only when the peer address of the member has the same type as the network interface address.

If you want to use a local IPv6 link address to establish BGP neighborship, you must use the local link address for the local device and peer. The BGP neighborship can be established only when the outbound interface address of the peer device is consistent with the local specified neighbor address. You can configure the same local link address for different interfaces. Therefore, you can but specify the interface name.

The local IPv6 link address can be used to establish only single-hop BGP neighborship.

Examples

The following example uses loopback 1 as a TCP source address during the establishment of a BGP connection with the peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.0.0.1 update-source loopback 1
```

Notifications

If the configured source address is invalid, the following notification will be displayed:

```
% Invalid host address: ipv4-address
```

If the source address of a peer group is configured as an IPv4 address, the following notification will be displayed:

```
% Source address %s is valid for IPv4 address members only
```

If the source address of a peer group is configured as an IPv6 address, the following notification will be displayed:

```
% Source address %s is valid for IPv6 address members only
```

If the neighbor relationship of a local link address is established and the local interface address is configured as the source address of a local link, the following notification will be displayed:

```
% % IPv6 link-local peer does not support IPv6 address as the update-source
```

If the source address is configured as a local IPv6 link address, the following notification will be displayed:

```
% Specify IPv6 link-local address as the update-source can't identify the only link
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.150 neighbor version

Function

Run the **neighbor version** command to configure the BGP version number for a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BGP version number is configured for a specified BGP peer.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **version 4**

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **version**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **version**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

4: Specifies the BGP version number as **4**.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 VRF address family of BGP

Configuration mode of the IPv6 VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, the version negotiation function of BGP becomes invalid.

Examples

The following example sets the BGP version number of peers to **4**.

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.1.1.1 version 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.151 neighbor weight

Function

Run the **neighbor weight** command to configure a weight value for a specified BGP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No weight value is configured for a specified BGP peer by default. The initial weight value of routes learned from neighbors is **0**, and the initial weight value of routes generated locally is **32768**.

Syntax

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **weight** *weight-value*

no neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **weight**

default neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **weight**

Parameter Description

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-group-name: Name of a specified peer group.

weight-value: Weight value of a neighbor. The value range is from 0 to 65535.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

After this command is configured, routes received from a specified neighbor use the specified value as the initial weight value. A greater weight value indicates a higher priority of a route.

Running the **set weight** command in the route map of a neighbor overwrites the configured weight value of this command.

Examples

The following example sets the weight value of routes received from the peer 10.1.1.1 to **73**.

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 10.1.1.1 weight 73
```

Notifications

If this neighbor is not activated in this address family, the following notification will be displayed:

```
% Activate the neighbor for the address family first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.152 network

Function

Run the **network** command to add static routing entries to a BGP routing table and advertise them to peers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static routing entry is added to a BGP routing table and advertised to peers by default.

Syntax

network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

no network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

default network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

Parameter Description

network-number: Network number.

mask: Subnet mask.

route-map *map-tag*: Specifies the name of a route map. The value cannot exceed 32 characters.

backdoor: Specifies the route as a backdoor route.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command allows IGP routes to be added to a BGP routing table. The advertised route information includes directly connected routes, static routes, and dynamic routes.

When this command is run, you can specify a route map. The route map allows you to modify the advertised route information.

Examples

The following example configures a BGP speaker to advertise the route 10.0.0.0/16.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# network 10.0.0.1 mask 255.255.0.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.153 network synchronization

Function

Run the **network synchronization** command to synchronize a device with the local route to advertise the routing information configured by the **network** command.

Run the **no** form of this command to configure a device to directly advertise the routing information configured by the **network** command, whether the local route is synchronized or not.

Run the **default** form of this command to restore the default configuration.

By default, a device synchronizes with the local route to advertise the routing information configured by the **network** command.

Syntax

network synchronization

no network synchronization

default network synchronization

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

You can run this command to modify the device action on the routing information configured by the **network** command in advertisement. You are not advised to configure a device to directly advertise routing information configured by the **network** command, because this may cause a route black hole.

Examples

The following example configures a BGP speaker to synchronize with the local route to advertise routing information configured by the **network** command.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# network synchronization
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.154 overflow memory-lack

Function

Run the **overflow memory-lack** command to configure BGP to enter the overflow state when the memory is insufficient.

Run the **no** form of this command to disable BGP from entering the overflow state when the memory is insufficient.

Run the **default** form of this command to restore the default configuration.

BGP enters the overflow state by default when the memory is insufficient.

Syntax

overflow memory-lack

no overflow memory-lack

default overflow memory-lack

Parameter Description

N/A

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

After entering the overflow state, BGP discards learned routes. This ensures that the memory does not increase.

After this command is run, a route loop may occur on the entire network if the BGP address family enters the overflow state and discards learned routes. To reduce the occurrence of this problem, BGP generates a default route toward the null interface. This route always exists in the overflow state.

You can run the **clear bgp** { *addressfamily* | **all** } command to reset the BGP session and clear the overflow state of the BGP address family.

You can run the **no** form of this command to disable BGP from entering the overflow state when the memory is insufficient. This may consume memory resources. When the memory usage exceeds the threshold of the software, all BGP neighbors are disconnected and all learned routes are removed.

Examples

The following example disables BGP from entering the overflow state when the memory is insufficient.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# no overflow memory-lack
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.155 redistribute

Function

Run the **redistribute** command to redistribute the routing information of another routing protocol to a BGP instance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No routing information of another routing protocol is redistributed to a BGP instance by default.

Syntax

redistribute *protocol-type* [**metric** *metric-value* | **route-map** *map-tag*] *

no redistribute *protocol-type* [**metric** | **route-map**] *

default redistribute *protocol-type* [**metric** | **route-map**] *

Parameter Description

protocol-type: Source protocol type of a redistributed route. The parameter can be set to one of the following values:

- **arp-host**: Specifies a host route converted from ARP.
- **connected**: Specifies a directly connected route.
- **rip**: Specifies an RIP route.
- **static**: Specifies a static route.

route-map *map-tag*: Specifies the name of an associated route map. No route map is associated by default.

metric *metric-value*: Specifies the default metric value for a redistributed route. The value range is from 0 to 4294967295.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If you specify an optional parameter during the configuration of the **no** form of this command, you remove only the configuration of the parameter, but do not remove the redistribution of routing information.

The metric values of routes are processed in the following order:

(1) If you work out a route map during the configuration of this command, the software applies the route map to process the metric value of a redistributed route. If you configure metric processing for the route map, you use the processed metric value.

(2) If you do not configure metric processing for the route or you only specify the **metric** parameter and *metric-value* during the configuration of this command, you use the *metric-value*.

(3) If no metric processing method is configured and no parameter is specified, the software directly uses the value of the redistributed route.

Examples

The following example configures BGP to redistribute static routes and filters the redistributed routes according to the route map static-rmap.

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# redistribute static route-map-name static-rmap
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.156 redistribute isis

Function

Run the **redistribute isis** command to redistribute the routing information of the IS-IS routing protocol to a BGP instance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No routing information of the IS-IS routing protocol is redistributed to a BGP instance by default.

Syntax

redistribute isis [*isis-tag*] [{ **level-1** | **level-1-2** | **level-2** } | **metric** *metric-value* | **route-map** *map-tag*] *
no redistribute isis [*isis-tag*] [{ **level-1** | **level-1-2** | **level-2** } | **metric** | **route-map**] *

default redistribute isis [*isis-tag*] [{ **level-1** | **level-1-2** | **level-2** } | **metric** | **route-map**] *

Parameter Description

isis-tag: Process name of a redistributed IS-IS route.

level-1: Redistributes only level 1 routing information of IS-IS.

level-1-2: Redistributes both level 1 and level 2 routing information of IS-IS.

level-2: Redistributes only level 2 routing information of IS-IS. This is the default configuration of IS-IS route redistribution.

metric: Configures the default metric value of a redistributed route.

metric-value: Default metric value of a redistributed route. The value range is from 0 to 4294967295.

route-map: Configures an associated route map. If this parameter is not specified, no route map is associated.

map-tag: Name of a route map.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If you specify an optional parameter during the configuration of the **no** form of this command, you remove only the configuration of the parameter, but do not remove the redistribution of routing information. After all subtypes of routes are deleted, the default type of routes are redistributed.

The IS-IS routes are filtered in the following order:

(1) First, IS-IS route types are filtered based on the configured **level** parameter.

(2) Then, they are filtered based on the rule of a route map.

The metric values of routes are processed in the following order:

(3) If you work out a route map during the configuration of this command, the software applies the route map to process the metric value of a redistributed route. If you configure metric processing for the route map, you use the processed metric value.

(4) If you do not configure metric processing for the route map or you only specify the **metric** parameter and *metric-value* during the configuration of this command, you use the *metric-value*.

(5) If no metric processing method is configured and no parameter is specified, the software directly uses the value of the redistributed route.

Examples

The following example configures BGP to redistribute IS-IS routes and filters the redistributed routes based on the route map static-rmap.

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# redistribute isis route-map-name static-rmap
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.157 redistribute ospf

Function

Run the **redistribute ospf** command to redistribute the routing information of the Open Shortest Path First (OSPF) routing protocol to a BGP instance.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No routing information of the OSPF routing protocol is redistributed to a BGP instance by default.

Syntax

redistribute ospf *process-id* [**match** { { **external** | { **external 1** | **external 2** }* } | **internal** | { **nssa-external** | { **nssa-external 1** | **nssa-external 2** } * } } * | **metric** *metric-value* | **route-map** *map-tag*] *

no redistribute ospf *process-id* [**match** { { **external** | { **external 1** | **external 2** }* } | **internal** | { **nssa-external** | { **nssa-external 1** | **nssa-external 2** } * } } * | **metric** | **route-map**] *

default redistribute ospf *process-id* [**match** { { **external** | { **external 1** | **external 2** }* } | **internal** | { **nssa-external** | { **nssa-external 1** | **nssa-external 2** } * } } * | **metric** | **route-map**] *

Parameter Description

process-id: Process ID of a redistributed OSPF route.

match: Specifies the subtype of a matched OSPF route.

external: Specifies the external types of OSPF routes, including type 1 and type 2.

external 1: Specifies the external type 1 of OSPF routes.

external 2: Specifies the external type 2 of OSPF routes.

internal: Specifies the internal subtype of OSPF routes, which is the default value of the **match** keyword for redistributed OSPF routes.

nssa-external: Specifies the NSSA external types of OSPF routes, including type 1 and type 2.

nssa-external 1: Specifies the NSSA external type 1 of OSPF routes.

nssa-external 2: Specifies the NSSA external type 2 of OSPF routes.

metric: Configures the default metric value of a redistributed route.

metric-value: Default metric value of a redistributed route. The value range is from 0 to 4294967295.

route-map: Configures an associated route map. If this parameter is not specified, no route map is associated.

map-tag: Name of a route map.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

If you specify an optional parameter during the configuration of the **no** form of this command, you remove only the configuration of the parameter, but do not remove the redistribution of routing information. After all subtypes of routes are deleted, the default type of routes are redistributed.

The OSPF routes are filtered in the following order:

(1) First, OSPF route types are filtered based on the configured **match** parameter.

(2) Then, they are filtered based on the rule of a route map.

The metric values of routes are processed in the following order:

(3) If you work out a route map during the configuration of this command, the software applies the route map to process the metric value of a redistributed route. If you configure metric processing for the route map, you use the processed metric value.

(4) If you do not configure metric processing for the route map or you only specify the **metric** parameter and *metric-value* during the configuration of this command, you use the *metric-value*.

(5) If no metric processing method is configured and no parameter is specified, the software directly uses the value of the redistributed route.

Examples

The following example configures BGP to redistribute routes of the OSPF process 2 and filters the redistributed routes based on the route map static-rmap.

```
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# redistribute ospf 2 route-map-name static-rmap
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.158 route mirroring

Function

Run the **route mirroring** command to enable the function of BGP packet mirroring.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of BGP packet mirroring is disabled by default.

Syntax

route mirroring

no route mirroring

default route mirroring

Parameter Description

N/A

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

Mirrored packets are sent to a BMP server. Mirroring BGP packets affects BGP performance.

Examples

The following example enables the function of BGP packet mirroring of BMP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# route mirroring
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.159 router bgp

Function

Run the **router bgp** command to enable the BGP protocol, configure a local AS number, and enter the BGP configuration mode.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

BGP is disabled by default.

Syntax

router bgp *as-number*

no router bgp *as-number*

default router bgp *as-number*

Parameter Description

as-number: AS number. A 4-byte AS number can be configured. That is, the new AS number range is from 1 to 4294967295, or from 1 to 65535.65535 in dot mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can configure this command to enable the BGP protocol.

RFC 4893 defines a newly reserved AS number 23456, and the number cannot be used as a private AS number. The value range of the original private AS numbers from 64512 to 65534 remains valid, and 65535 is reserved for special purposes.

RFC 5398 defines two groups of AS numbers, their value ranges are from 64496 to 64511 and from 65536 to 65551.

Examples

The following example enables the BGP protocol and sets the local AS number to **65000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.160 scope

Function

Run the **scope** command to enter the scope configuration mode and associate a VRF instance with BGP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No scope address family is configured by default.

Syntax

scope vrf *vrf-name*

no scope vrf *vrf-name*

default scope vrf *vrf-name*

Parameter Description

vrf *vrf-name*: VRF name.

Command Modes

BGP configuration mode

Default Level

14

Usage Guidelines

You can run the **exit** command to exit the scope configuration mode.

Note

In the scope configuration mode, commands configured in the BGP configuration mode are converted to scope command mode. To restore the scope command mode to the original command mode, you can configure the **no router bgp** command and reconfigure the commands.

Examples

The following example enters the scope VRF configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# scope vrf VRF
Hostname(config-router-scope)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.161 show bgp all

Function

Run the **show bgp all** command to display all the routing information of BGP.

Syntax

show bgp all [**aggregate** | **community** [*community-number* [**exact-match**]] | **community-list** *community-name*&<1-n> [**extact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **inconsistent-as** | **quote-regexp** *regexp* | **regexp** *regexp*]

show bgp all dampening { **dampened**-**paths** | **flap**-**statistics** | **parameters** }

show bgp all neighbors [{ *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**advertised**-**routes** [**check**] | **ha-mode** [**adj-in** [**detail**] | **adj-out**] | **hide-info** | **policy** [**detail**] | **received**-**routes** | **routes**]]

show bgp all paths

show bgp all summary

show bgp all update-**group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**ha-mod adj-out** | **summary**]

Parameter Description

aggregate: Displays the routing aggregation information.

community: Displays the routing information that contains the specified community number.

community-number: Specified community number. This parameter can be entered for multiple times. This parameter follows the format of AA:NN (AS number: 2-byte number) or is set to one of the following community names:

- **gshut**
- **internet**
- **local-as**
- **no-advertise**
- **no-export**

exact-match: Specifies the routing information that exactly matches community values or a community list.

community-list *community-name*: Displays the BGP routing information that matches a specified community list. *community-name* specifies the name of a community list.

extcommunity-list *extcommunity-name*: Displays the BGP routing information that contains the name of a specified extended community list or the number of a community list. *extcommunity-name* specifies the name of an extended community list or the number of a community list.

filter-list *path-list-number*: Displays the routing information that matches the filtering list. *path-list-number* is the number of a filtering list. The value range is from 1 to 500.

inconsistent-as: Displays the inconsistent routing information of the source AS.

quote-regexp *regexp*: Displays the BGP routing information that matches a regular expression within the specified double quotation marks in the AS-PATH attribute.

regexp *regexp*: Displays the BGP routing information that matches a specified regular expression in the AS-PATH attribute.

dampening: Displays route suppression information.

dampened-paths: Displays suppressed routing information.

flap-statistics: Displays route flapping statistics.

parameters: Displays route flapping parameters.

neighbors: Displays BGP neighbor information.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

advertised-routes: Displays all the routing information sent to a specified peer.

check: Displays route filtering debugging information.

hide-info: Displays BGP NSR information.

adj-in: Displays the routing information received by the BGP neighbor NSR.

detail: Displays detailed information.

adj-out: Displays the routing information sent by the BGP neighbor NSR.

hide-info: Displays internal information.

policy: Displays the routing policy information about the BGP neighbor.

received-routes: Displays all the routing information received from a specified peer, including received routes and rejected routes.

routes: Displays all the routing information received from peers.

paths: Displays the routing information in a routing information base.

summary: Displays BGP neighbor information.

update-group: Displays update group information.

update-group-index: Index of a specified update group.

ha-mod adj-out: Displays the routing information sent by the BGP neighbor NSR.

summary: Displays summary information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to display all the family address information in the BGP routing information.

Examples

The following example displays all neighbor information.

```
Hostname> enable
Hostname# show bgp all
For address family: IPv4 Unicast
BGP table version is 1, local router ID is 1.2.3.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf     Weight Path
*> 1.0.0.0          0.0.0.0                  0                32768    ?
Total number of prefixes 1
For address family: IPv6 Unicast
BGP table version is 1, local router ID is 1.2.3.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf     Weight Path
*> 5750:1::/120     ::                       0                32768    ?
Total number of prefixes 1
```

Table 1-1 Output Fields of the show bgp all Command

Field	Description
For address family	BGP address family information
BGP table version	BGP table version
local router ID	Local router ID, which is a loopback address generally
Status codes	Status code of a BGP route
s	Suppressed route
d	Route flapping shielding
h	Historic route, unavailable route
*	Valid route
>	Optimal route

Field	Description
i	IBGP route
r	RIB failed to install a routing table
S	Stale route
Origin Codes	Original code of a BGP route
i	IGP originating route in a BGP routing table
e	EGP originating route in a BGP routing table
?	Unable to determine the source of a route in a BGP routing table
Network	Network routing information in the format of aa:bb. aa specifies a site ID and bb specifies a label block offset.
Next hop	IP address of a next hop
Metric	Metric value of a route
LocPrf	Local priority
Weight	Weight. The weight of a locally generated route is 32768.
Path	AS path that reaches the destination network

Notifications

N/A

Platform Description

N/A

1.162 show bgp bmp

Function

Run the **show bgp bmp** command to display BMP server information.

Syntax

show bgp bmp { **neighbor** | **server** [*server-number*] [**detail**] | **summary** }

Parameter Description

neighbor: Displays the neighbors monitored by a BMP server.

server: Displays BMP server instance information.

server-number: ID of a specified BMP server instance.

detail: Displays the detailed information of a BMP server instance.

summary: Display the summary information about connection establishment of a BMP server.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the BMP server instance information.

```
Hostname> enable
Hostname# show bgp bmp server 1
BMP server 1
  BMP state = Idle
  up time       Never
  BGP monitor neighbors: 4
  route mirroring
```

The following example displays the neighbors monitored by a BMP server.

```
Hostname> enable
Hostname# show bgp bmp neighbor
Neighbor       CfgSvr#          ActSvr#
3.3.3.1        1               1
3.3.3.2        1               1
```

Table 1-2 Output Fields of the show bgp bmp neighbor Command

Field	Description
Neighbor	Address of a monitored neighbor
CfgSvr#	Instance ID of the configured BMP server that monitors this neighbor
ActSvr#	Instance ID of the BMP server that is activated to monitor this neighbor

The following example displays the summary information about connection establishment of a BMP server.

```
Hostname> enable
Hostname# show bgp bmp summary
ID   Host               Port     State       Time       NBRs
1    123.123.123.123     12345    Active      Never      4
```

Table 1-3 Output Fields of the show bgp bmp summary Command

Field	Description
ID	Address of a monitored neighbor

Field	Description
Host	Instance ID of the configured BMP server that monitors this neighbor
Port	Listening port of a BMP server
State	Connection state of a BMP server
Time	Connection or disconnection time of a BMP server
NBRs	Number of neighbors monitored by a BMP server

Notifications

N/A

Platform Description

N/A

1.163 show bgp develop

Function

Run the **show bgp develop** command to display the development information of BGP.

Syntax

show bgp develop { **bgp-instance** | **cap** | **connected** | **evi-rd-hash** | **ifx-link-group** | **interface nd** [*ifx-number*] | **io-process** [**log-info** | **log-warn** | **master** | **memory** | **peer** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-id*]] | **link-state-group** | **mom** | **peer-as** | **pic-info** | **route-shake** | **thread** | **vr** | **vrf-rd-hash** }

Parameter Description

bgp-instance: Displays specific information of a BGP instance.

cap: Displays state information of a BGP capability.

connected: Displays BGP neighbor connection information.

evi-rd-hash: Displays RD information of all EVI instances.

ifx-link-group: Displays link group information.

interface nd: Displays IPv6 neighbor information.

ifx-number: Interface IFX number. The value range is from 1 to 16777215.

io-process: Displays all IO processes or a single IO process.

log-info: Displays the log information of all IO processes or a single IO process.

log- warn: Displays the alarm information of all IO processes or a single IO process.

master: Displays the main information of all IO processes or a single IO process.

memory: Displays the memory information of all IO processes or a single IO process.

peer: Displays the IO statistics about a peer.

neighbor-ipv4-address: IPv4 address of a specified peer.

neighbor-ipv6-address: IPv6 address of a specified peer.

peer-id: ID of a specified peer.

link-state-group: Displays the BGP link state group information.

mom: Displays the MOM connection state.

peer-as: Displays the number of neighbors.

pic-info: Displays the PIC information of BGP.

route-shake: Displays the route flapping information.

thread: Displays all BGP thread information.

vr: Displays global VR details.

vrf-rd-hash: Displays the VRF RD information of BGP.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to locate faults.

Examples

The following example displays the RD information of all VRF instances.

```
Hostname> enable
Hostname# show bgp develop vrf-rd-hash
VRF RD Hash:
  rd: 2:2, owner: VRF(v2)
  rd: 1:1, owner: VRF(v1)
```

Notifications

N/A

Platform Description

N/A

1.164 show bgp grst

Function

Run the **show bgp grst** command to display GR information.

Syntax

show bgp grst { **bfd** | **label** | **label-set** | **mdc** | **peer-info** | **status** }

Parameter Description

bfd: Displays the BFD information of neighbors.

label: Displays label information.

label-set: Displays the set label information.

mdc: Displays Multicast Distribution Controller (MDC) information.

peer-info: Displays neighbor information.

status: Displays the GR state.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.165 show bgp hash-peer

Function

Run the **show bgp hash-peer** command to display the hash table information of all neighbors.

Syntax

show bgp hash-peer

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the hash table information of all neighbors.

```
Hostname> enable
Hostname# show bgp hash-peer
peer address hash table:
 vrf_id        prefix                      peer
 0            172.20.91.118                172.20.91.118
 0            10.0.0.3                    10.0.0.3
 0            10.0.0.5                    10.0.0.5
```

Notifications

N/A

Platform Description

N/A

1.166 show bgp ipv4 unicast

Function

Run the **show bgp ipv4 unicast** command to display the IPv4 unicast routing information in BGP routing information.

Syntax

show bgp ipv4 unicast [*prefix-ipv4-address* [*network-mask* [**longer-prefixes**]] | **aggregate** | **cidr-only** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **global-vrf detail** | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]

show bgp ipv4 unicast vrf *vrf-name* [*prefix-ipv4-address* [*network-mask* [**longer-prefixes**]] | **aggregate** | **cidr-only** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]]

Parameter Description

prefix-ipv4-address: IPv4 address of a specified prefix.

network-mask: Mask of a specified network prefix.

longer-prefixes: Displays the specific routing information included in a specified prefix.

aggregate: Displays the detailed information of an aggregate route.

cidr-only: Displays the classless routing information.

community: Displays the routing information that contains the specified community number.

community-number&<1-n>: Specified community number. &<1-n> specifies that this parameter can be entered *n* times. This parameter follows the format of AA:NN (AS number: 2-byte number) or is set to one of the following community names:

- **gshut**
- **internet**
- **local-as**
- **no-advertise**
- **no-export**

exact-match: Specifies the routing information that exactly matches community values or a community list.

community-list *community-name*: Displays the BGP routing information that matches a specified community list. *community-name* specifies the name of a community list.

extcommunity-list *extcommunity-name*: Displays the BGP routing information that contains the name of a specified extended community list or the number of a community list. *extcommunity-name* specifies the name of an extended community list or the number of a community list.

filter-list *path-list-number*: Displays the routing information that matches the filtering list. *path-list-number* is the number of the filtering list. The value range is from 1 to 500.

global-vrf detail: Displays global VRF information.

inconsistent-as: Displays the inconsistent routing information of the source AS.

prefix-list *ip-prefix-list-name*: Displays the routing information that matches a specified prefix filtering list.

quote-regexp *regexp*: Displays the routing information that matches a regular expression within the specified double quotation marks in the AS-PATH attribute.

regexp *regexp*: Displays the routing information that matches a specified regular expression in the AS-PATH attribute.

route-map *map-tag*: Displays the routing information that matches the filtering condition of a specified route map. *map-tag*: Name of a route map.

vrf *vrf-name*: Specifies a VRF name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can use this command to display the BGP IPv4 unicast routing information. By specifying parameters, you can filter routing information that matches the specified conditions.

Examples

The following example displays the routing information of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network         Next Hop             Metric     LocPrf  Path
*>i44.0.0.0         192.168.195.183         0        100     i
*>i64.12.0.0/16     192.168.195.183         0        100     i
*>i172.16.0.0/24    192.168.195.183         0        100     i
*>i202.201.0.0      192.168.195.183         0        100     i
*>i202.201.1.0      192.168.195.183         0        100     i
*>i202.201.2.0      192.168.195.183         0        100     i
*>i202.201.3.0      192.168.195.183         0        100     i
*>i202.201.18.0     192.168.195.183         0        100     i
Total number of prefixes 8
```

The following example displays the BGP IPv4 routing information that contains the specified community attributes.

```
Hostname> enable
Hostname# show bgp ipv4 unicast community 11:2222
111:12345
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop             Metric     LocPrf  Path
*>i202.201.0.0      192.168.195.183         0        100     i
*>i202.201.1.0      192.168.195.183         0        100     i
*>i202.201.2.0      192.168.195.183         0        100     i
*>i202.201.3.0      192.168.195.183         0        100     i
Total number of prefixes 4
```

The following example displays the BGP IPv4 routing information that matches the filtering conditions.

```
Hostname> enable
Hostname# show bgp ipv4 unicast filter-list 5
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf  Path
*>192.168.88.0       0.0.0.0              32768 ?
Total number of prefixes 1
```

The following example displays the classless routing information in BGP IPv4 routing information.

```
Hostname> enable
Hostname# show bgp ipv4 unicast cidr-only
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop             Metric     LocPrf  Path
*>i64.12.0.0/16     192.168.195.183         0        100     i
*>i172.16.0.0/24    192.168.195.183         0        100     i
```

```
Total number of prefixes 2
```

Table 1-4 Output Fields of the show bgp ipv4 unicast Command

Field	Description
BGP table version	BGP table version
local router ID	Local router ID, which is a loopback address generally
Status codes	Status code of a BGP route
s	Suppressed route
d	Route flapping shielding
h	Historic route, unavailable route
*	Valid route
>	Optimal route
i	IBGP route
S	Stale route
Origin Codes	Original code of a BGP route
i	IGP originating route in a BGP routing table
e	EGP originating route in a BGP routing table
?	Unable to determine the source of a route in a BGP routing table
Network	Network routing information in the format of aa:bb. aa specifies a site ID and bb specifies a label block offset.
Next hop	IP address of a next hop
Metric	Metric value of a route
LocPrf	Local priority
Path	AS path that reaches the destination network

Notifications

N/A

Platform Description

N/A

1.167 show bgp ipv4 unicast dampening

Function

Run the **show bgp ipv4 unicast dampening** command to display the BGP IPv4 unicast route flapping information.

Syntax

show bgp ipv4 unicast [**vrf** *vrf-name*] **dampening** { **dampened-paths** | **flap-statistics** | **parameters** }

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

dampened-paths: Displays the suppressed routes in the IPv4 routing information of BGP.

flap-statistics: Displays the route flapping statistics in the IPv4 routing information of BGP.

parameters: Displays the parameters of the IPv4 unicast route flapping information configured by BGP.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the parameters of an IPv4 unicast route flapping information of BGP.

Examples

The following example displays the route flapping and damping parameters of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast dampening parameters
dampening 10 750 2000 40
Dampening Control Block(s):
Reachability Half-Life time    : 10 min
Reuse penalty                : 750
Suppress penalty             : 2000
Max suppress time            : 40 min
Max penalty (ceil)           : 12000
```

Table 1-5 Output Fields of the show bgp ipv4 unicast dampening parameters Command

Field	Description
dampening	Route flapping parameter
Reachability Half-Life time	Half-life time
Reuse penalty	A route is damped when the penalty is reduced to this value.

Field	Description
Suppress penalty	A route is damped when the penalty reaches this value.
Max suppress time	Maximum route suppression time
Max penalty (ceil)	Maximum penalty

Notifications

N/A

Platform Description

N/A

1.168 show bgp ipv4 unicast neighbors

Function

Run the **show bgp ipv4 unicast neighbors** command to display the IPv4 unicast neighbor information of BGP.

Syntax

show bgp ipv4 unicast [**vrf** *vrf-name*] **neighbors** [{ *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**advertised-routes** [**check**] | **ha-mode** [**adj-in** [**detail**] | **adj-out**] | **hide-info** | **policy** [**detail**] | **received-routes** | **routes**]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

advertised-routes: Displays all the routing information sent to a specified peer.

check: Displays route filtering debugging information.

ha-mode: Displays BGP NSR information.

adj-in: Displays the routing information received by the BGP neighbor NSR.

detail: Displays detailed information.

adj-out: Displays the routing information sent by the BGP neighbor NSR.

hide-info: Displays internal information.

policy: Displays the routing policy information about the BGP neighbor.

received-routes: Displays all the routing information received from a specified peer, including received routes and rejected routes.

routes: Displays all the routing information received from peers.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IPv4 unicast neighbor connection information of BGP.

Examples

The following example displays the neighbor information of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast neighbors
BGP neighbor is 192.168.195.183, remote AS 23, local AS 23, internal link
  BGP version 4, remote router ID 44.0.0.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
Remote Restart timer is 120 seconds
  Received 14 messages, 0 notifications, 0 in queue
    open message:1 update message:4 keepalive message:9
    refresh message:0 dynamic cap:0 notifications:0
  Sent 12 messages, 0 notifications, 0 in queue
    open message:1 update message:3 keepalive message:8
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Inbound soft reconfiguration allowed
  8 accepted prefixes
  0 announced prefixes
 Connections established 2; dropped 1
Local host: 192.168.195.239, Local port: 1074
Foreign host: 192.168.195.183, Foreign port: 179
Nexthop: 192.168.195.239
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:06:43, due to BGP Notification sent
Notification Error Message: (Cease/Unspecified Error Subcode)
Using BFD to detect fast fallover
```

Table 1-6 Output Fields of the show bgp ipv4 unicast neighbors Command

Field	Description
BGP neighbor	Address of a BGP peer
remote AS	Remote AS number
local AS	Local AS number
internal link	IBGP peer
BGP version	BGP version number after negotiation
remote router ID	Router ID of remote BGP
BGP state	State machine state of a peer
Neighbor capabilities	Capability negotiation state of a peer
For address family: IPv4 Unicast	Statistics about IPv4 unicast address family of a peer

Notifications

N/A

Platform Description

N/A

1.169 show bgp ipv4 unicast paths

Function

Run the **show bgp ipv4 unicast paths** command to display the IPv4 unicast path information in a routing information base.

Syntax

show bgp ipv4 unicast [**vrf** *vrf-name*] **paths**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the path information in a routing database.

Examples

The following example displays the path information of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast paths
Address       Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Table 1-7 Output Fields of the show bgp ipv4 unicast paths Command

Field	Description
Address	Memory address of an AS path
Refcnt	Reference count of an AS path
Path	AS path information

Notifications

N/A

Platform Description

N/A

1.170 show bgp ipv4 unicast summary

Function

Run the **show bgp ipv4 unicast summary** command to display the BGP IPv4 unicast summary information.

Syntax

show bgp ipv4 unicast [**vrf** *vrf-name*] **summary**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the BGP IPv4 unicast neighbor information.

Examples

The following example displays the neighbor summary information of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor        V    AS   MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.195.79   4    24     0       0       0     0    0    never      Active
192.168.195.183  4    23     17      15      1     0    0    00:09:04    8
Total number of neighbors 2
```

Table 1-8 Output Fields of the show bgp ipv4 unicast summary Command

Field	Description
BGP router identifier	Router ID of BGP
local AS number	Local AS number of BGP
BGP table version	Routing table version of BGP
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version number
AS	Remote AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	State machine state of a neighbor or number of received route entries

Notifications

N/A

Platform Description

N/A

1.171 show bgp ipv4 unicast update-group

Function

Run the **show bgp ipv4 unicast update-group** command to display the BGP IPv4 unicast update group information.

Syntax

show bgp ipv4 unicast [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**ha-mod adj-out** | **summary**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

update-group-index: Specific update group information.

ha-mod adj-out: Displays the routing information sent by the BGP neighbor NSR.

summary: Displays neighbor summary information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the BGP IPv4 unicast update group information.

Examples

The following example displays the update group information of an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 update-group
BGP version 4 update-group 1(ref 2), internal, Address Family: IPv4 Unicast
  Update message formated 2, replicated 2
  Minimum route advertisement interval is 0 seconds
  Minimum AS origination interval is 1 seconds
  Format state: Current working
              Refresh blocked
  Has 1 members:
   192.168.195.183
```

Table 1-9 Output Fields of the show bgp ipv4 unicast update-group Command

Field	Description
BGP version	BGP version number
update-group	BGP route update group
internal	IBGP route
Address Family	Address family information
Update message formated	Format of an update message

Field	Description
replicated	Replicate message
Minimum route advertisement interval	Minimum route advertisement interval
Minimum AS origination interval	Minimum sending interval of an update message in which the AS route of the BGP speaker resides changes
Format state	Format state
members	Neighbor information

The following example displays the neighbor summary information of update group 1 in an IPv4 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv4 unicast update-group 1 summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor        V    AS   MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.195.79   4    24     0       0       0    0    0    never      Active
192.168.195.183  4    23     17      15      1    0    0    00:09:04    8
Total number of neighbors 2
```

Table 1-10 Output Fields of the show bgp ipv4 unicast update-group 1 summary Command

Field	Description
BGP router identifier	Router ID of BGP
local AS number	Local AS number of BGP
BGP table version	Routing table version of BGP
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version number
AS	Remote AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	State machine state of a neighbor or number of received route entries

Notifications

N/A

Platform Description

N/A

1.172 show bgp ipv6 unicast

Function

Run the **show bgp ipv6 unicast** command to display the IPv6 unicast routing information in BGP routing information.

Syntax

show bgp ipv6 unicast [*prefix-ipv6-address/prefix-length* [**longer-prefixes**] | **aggregate** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **global-vrf detail** | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]]

show bgp ipv6 unicast vrf *vrf-name* [*prefix-ipv6-address/prefix-length* [**longer-prefixes**] | **aggregate** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]

Parameter Description

prefix-ipv6-address/prefix-length: Specific IPv6 route prefix in a routing table.

longer-prefixes: Displays the specific routing information included in a specified prefix.

aggregate: Displays the detailed information of an aggregate route.

community: Displays the routing information that contains the specified community number.

community-number&<1-n>: Specified community number. &<1-n> specifies that this parameter can be entered *n* times. This parameter follows the format of AA:NN (AS number: 2-byte number) or is set to one of the following community names:

- **gshut**
- **internet**
- **local-as**
- **no-advertise**
- **no-export**

exact-match: Specifies the routing information that exactly matches community values or a community list.

community-list *community-name*: Displays the BGP routing information that matches a specified community list. *community-name* specifies the name of a community list.

extcommunity-list *extcommunity-name*: Displays the BGP routing information that contains the name of a specified extended community list or the number of a community list. *extcommunity-name* specifies the name of an extended community list or the number of a community list.

filter-list *path-list-number*: Displays the routing information that matches the filtering list. *path-list-number* is the number of a filtering list. The value range is from 1 to 500.

global-vrf detail: Displays the global VRF information.

inconsistent-as: Displays the inconsistent routing information of the source AS.

prefix-list *ip-prefix-list-name*: Displays the routing information that matches a specified prefix filtering list.

quote-regexp *regexp*: Displays the routing information that matches a regular expression within the specified double quotation marks in the AS-PATH attribute.

regexp *regexp*: Displays the routing information that matches a specified regular expression in the AS-PATH attribute.

route-map *map-tag*: Displays the routing information that matches the filtering condition of a specified route map. *map-tag*: Name of a route map.

vrf *vrf-name*: Specifies a VRF name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to display the IPv6 unicast routing information of BGP. By specifying parameters, you can filter the routing information that matches the specified conditions.

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.173 show bgp ipv6 unicast dampening

Function

Run the **show bgp ipv6 unicast dampening** command to display the IPv6 unicast route flapping parameters configured by BGP.

Syntax

show bgp ipv6 unicast [**vrf** *vrf-name*] **dampening** { **dampened-paths** | **flap-statistics** | **parameters** }

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

dampened-paths: Displays the suppressed routes in the BGP IPv6 routing information.

flap-statistics: Displays the route flapping statistics in the BGP IPv6 routing information.

parameters: Displays the IPv6 unicast route flapping parameters configured by BGP.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the parameters of the BGP IPv6 unicast route flapping information.

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.174 show bgp ipv6 unicast neighbors

Function

Run the **show bgp ipv6 unicast neighbors** command to display the IPv6 unicast neighbor information of BGP.

Syntax

show bgp ipv6 unicast [**vrf** *vrf-name*] **neighbors** [{ *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**advertised-routes** [**check**] | **ha-mode** [**adj-in** [**detail**] | **adj-out**] | **hide-info** | **policy** [**detail**] | **received-routes** | **routes**]]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

advertised-routes: Displays all the routing information sent to a specified peer.

check: Displays route filtering debugging information.

ha-mode: Displays BGP NSR information.

adj-in: Displays the routing information received by the BGP neighbor NSR.

detail: Displays detailed information.

adj-out: Displays the routing information sent by the BGP neighbor NSR.

hide-info: Displays internal information.

policy: Displays the routing policy information about the BGP neighbor.

received-routes: Displays all the routing information received from a specified peer, including received routes and rejected routes.

routes: Displays all the routing information received from peers.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IPv6 unicast neighbor connection information of BGP.

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.175 show bgp ipv6 unicast paths

Function

Run the **show bgp ipv6 unicast paths** command to display the IPv6 unicast path information in a routing information base.

Syntax

show bgp ipv6 unicast [**vrf** *vrf-name*] **paths**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the path information in a routing database.

Examples

The following example displays the path information of an IPv6 unicast address family of BGP.

```
Hostname> enable
```

```
Hostname# show bgp ipv6 unicast paths
Address          Refcnt Path
[0x1d7806a0:0]   (67)
[0x1d7389a0:13]  (20)   10
```

Table 1-11 Output Fields of the show bgp ipv6 unicast paths Command

Field	Description
Address	Memory address of an AS path
Refcnt	Reference count of an AS path
Path	AS path information

Notifications

N/A

Platform Description

N/A

1.176 show bgp ipv6 unicast summary

Function

Run the **show bgp ipv6 unicast summary** command to display the BGP IPv6 unicast summary information.

Syntax

show bgp ipv6 unicast [**vrf** *vrf-name*] **summary**

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the BGP IPv6 unicast neighbor information.

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.177 show bgp ipv6 unicast update-group

Function

Run the **show bgp ipv6 unicast update-group** command to display the BGP IPv6 unicast update group information.

Syntax

show bgp ipv6 unicast [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**ha-mod adj-out** | **summary**]

Parameter Description

vrf *vrf-name*: Specifies a VRF name. If this parameter is not specified, all VRF instances are specified.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

update-group-index: Specific update group information.

ha-mod adj-out: Displays the routing information sent by the BGP neighbor NSR.

summary: Displays neighbor summary information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IPv6 unicast update group information of BGP.

Examples

The following example displays the update group information of an IPv6 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv6 update-group
BGP version 4 update-group 1(ref 2), internal, Address Family: IPv6 Unicast
  Update message formated 2, replicated 2
  Minimum route advertisement interval is 0 seconds
  Minimum AS origination interval is 1 seconds
  Format state: Current working
              Refresh blocked
  Has 1 members:
   192:168:195::183
```

Table 1-12 Output Fields of the show bgp ipv6 update-group Command

Field	Description
BGP version	BGP version number
update-group	BGP route update group
internal	IBGP route
Address Family	Address family information
Update message formated	Format of an update message
replicated	Replicate message
Minimum route advertisement interval	Minimum route advertisement interval
Minimum AS origination interval	Minimum sending interval of an update message in which the AS route of the BGP speaker resides changes
Format state	Format state
members	Neighbor information

The following example displays the neighbor summary information of update group 1 in an IPv6 unicast address family of BGP.

```
Hostname> enable
Hostname# show bgp ipv6 unicast update-group 1 summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor        V    AS   MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192:168:195::79   4    24     0       0       0     0    0    never      Active
192:168:195::183  4    23     17      15      1     0    0    00:09:04    8
Total number of neighbors 2
```

Table 1-13 Output Fields of the show bgp ipv6 unicast update-group 1 summary Command

Field	Description
BGP router identifier	Router ID of BGP
local AS number	Local AS number of BGP
BGP table version	Routing table version of BGP
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address

Field	Description
V	Protocol version number
AS	Remote AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	State machine state of a neighbor or number of received route entries

Notifications

N/A

Platform Description

N/A

1.178 show bgp log-info

Function

Run the **show bgp log-info** command to display BGP log information.

Syntax

show bgp log-info

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BGP log information.

```
Hostname> enable
Hostname# show bgp log-info
************  start to print LOG in file
"/tmp/vsd/0/ucast/bgp/debug_info.log0new"***********.
```

Notifications

N/A

Platform Description

N/A

1.179 show bgp log-warn

Function

Run the **show bgp log-warn** command to display BGP alarm information.

Syntax

show bgp log-warn

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BGP alarm information.

```
Hostname> enable
Hostname# show bgp log-warn
************  start to print LOG in file
"/data/.rgos/vsd/0/ucast/bgp/debug_warn.log0"***********.
*Aug 28 2019 03:20:30.825: :[WARN][@bgp_unset_sysha-162] [BGP-SYSHA]: echo -17 >
/proc/4925/oom_adj
*Aug 28 2019 03:20:30.825: :[WARN][@bgp_unset_sysha-171] [BGP-SYSHA]: echo -1000 >
/proc/4925/oom_score_adj
*Aug 28 2019 03:20:35.508: :[WARN][@bgp_nsm_recv_nsr_aa_cap-5058] [MOM]: nsm to bgp
nsr aa.
*Aug 28 2019 03:24:11.693: :[WARN][@bgp_ha_sync_req_check-5463] [BGP-WARN]: Lib ha
sync is not ready.
*Aug 28 2019 03:24:17.162: :[WARN][@bgp_nsm_recv_nsr_aa_cap-5064] [MOM]: nsm to bgp
nsr as.
```

Notifications

N/A

Platform Description

N/A

1.180 show bgp memory

Function

Run the **show bgp memory** command to display BGP memory information.

Syntax

show bgp memory

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BGP memory information.

```
Hostname> enable
Hostname# show bgp memory
memory statistics:
name                 malloc     free       inuse      max        min
TMP                  456        55         401        2112       4
HASH                 82         0          82         40         40
HASH_INDEX           82         0          82         8192       1024
HASH_BUCKET          111        4          107        24         24
LINK_LIST            2815       2444       371        40         40
LIST_NODE            2567       2444       123        24         24
PREFIX_IPV4          6          0          6          8          8
PREFIX_IPV6          4          0          4          20         20
ROUTE_TABLE          18         0          18         16         16
ROUTE_NODE           87         0          87         96         96
LS_TABLE             100        0          100        24         24
VECTOR               117        0          117        16         16
VECTOR_INDEX         117        0          117        4096       8
SNMP_SUBTREE         5          0          5          544        544
SMUX_MIBMAP          1          1          0          536        536
CONFIG               1          0          1          2          2
CONFIG_MOTD          1          0          1          100        100
IF                   15         0          15         368        368
```

Notifications

N/A

Platform Description

N/A

1.181 show bgp nsr

Function

Run the **show bgp nsr** command to display NSR information.

Syntax

show bgp nsr { **info** | **sock-cb** [*sock-cb-id*] | **sock-list** | **status** }

Parameter Description

info: Displays NSR basic information.

sock-cb: Displays the socket CB information of BGP.

sock-cb-id: Specified socket CB information of BGP. The value range is from 0 to 4294967295.

sock-list: Displays saved socket handle information.

status: Displays NSR state information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.182 show bgp route-block

Function

Run the **show bgp route-block** command to display black hole route statistics.

Syntax

show bgp route-block

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays black hole route statistics.

```
Hostname> enable
Hostname# show bgp route-block
wait for controller: 0
 recv controller msg: 0
BGP NSM route block message information:
 recv route block count:0
 recv route unblock count:0
 recv route block max time:0
 recv route block last time:0
BGP self route block message information:
 recv self route block count:0
 recv self route unblock count:0
 size in: 0
 to recv: 0
 send msg count: 59
 recv msg count: 0
 send queue len: 0
```

Notifications

N/A

Platform Description

N/A

1.183 show bgp rpi

Function

Run the **show bgp rpi** command to display RPI policy information.

Syntax

show bgp rpi { **acl** [**detail**] | **as-path-access-list** | **community-list** | **extcommunity-list** | **ip-prefix-list** | **ipv6-prefix-list** | **route-map** }

Parameter Description

acl: Displays the ACL information of an RPI policy.

detail: Displays the ACL details of an RPI policy.

as-path-access-list: Displays the AS path information of an RPI policy.

community-list: Displays the attribute configuration information of an RPI policy.

extcommunity-list: Displays the extended attribute configuration information of an RPI policy.

ip-prefix-list: Displays the IPv4 route filtering information of an RPI policy.

ipv6-prefix-list: Displays the IPv6 route filtering information of an RPI policy.

route-map: Displays the route map information of an RPI policy.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.184 show bgp statistics

Function

Run the **show bgp statistics** command to display BGP statistics.

Syntax

show bgp statistics [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Displays the BGP statistics of a VRF instance. If this parameter is not specified, global BGP statistics information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BGP statistics.

```
Hostname> enable
Hostname# show bgp statistics
Local as 100, Router id 1.1.1.1
  Total neighbor 10, Established neighbor 9, Admin-Down neighbor 1
  IBGP neighbor 8, Established IBGP neighbor 8, Admin-Down IBGP neighbor 0
  EBGP neighbor 2, Established EBGP neighbor 1, Admin-Down EBGP neighbor 1
  AS-PATH entries 1, Community entries 1, Extended-Community entries 0
  For address family: IPv4 Unicast
Activated neighbor 9, Unactivated neighbor 0
Activated IBGP neighbor 8, Unactivated IBGP neighbor 0
Activated EBGP neighbor 1, Unactivated EBGP neighbor 0
  For address family: IPv6 Unicast
Activated neighbor 0, Unactivated neighbor 9
Activated IBGP neighbor 0, Unactivated IBGP neighbor 0
Activated EBGP neighbor 0, Unactivated EBGP neighbor 0
```

Table 1-14 Output Fields of the show bgp statistics Command

Field	Description
Router id	BGP router ID
Total neighbor	Total number of neighbors
Established neighbor	Number of established neighbors
Admin-Down neighbor	Number of admin-down neighbors
IBGP neighbor	Number of IBGP neighbors
Established IBGP neighbor	Number of established IBGP neighbors
Admin-Down IBGP neighbor	Number of admin-down IBGP neighbors
EBGP neighbor	Number of EBGP neighbors
AS-PATH entries	Number of AS-PATH entries
Community entries	Number of community entries

Field	Description
Extended-Community	Number of extended community entries
Established EBGP neighbor	Number of established EBGP neighbors
Admin-Down EBGP neighbor	Number of admin-down EBGP neighbors
Activated neighbor	Number of activated neighbors
Unactivated neighbor	Number of unactivated neighbors, excluding unestablished neighbors
Activated IBGP neighbor	Number of activated IBGP neighbors
Unactivated IBGP neighbor	Number of unactivated IBGP neighbors, excluding unestablished neighbors
Activated EBGP neighbor	Number of activated EBGP neighbors
Unactivated EBGP neighbor	Number of unactivated EBGP neighbors, excluding unestablished neighbors

Notifications

N/A

Platform Description

N/A

1.185 show ip bgp

Function

Run the **show ip bgp** command to display the routing information of an IPv4 unicast address family of BGP.

Syntax

show ip bgp [*prefix-ipv4-address* [*network-mask* [**longer-prefixes**]] | **aggregate** | **cidr-only** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **global-vrf detail** | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]

show ip bgp vrf *vrf-name* [*prefix-ipv4-address* [*network-mask* [**longer-prefixes**]] | **aggregate** | **cidr-only** | **community** [*community-number*&<1-n> [**exact-match**]] | **community-list** *community-name* [**exact-match**] | **extcommunity-list** *extcommunity-name* [**exact-match**] | **filter-list** *path-list-number* | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-tag*]]

show ip bgp [**vrf** *vrf-name*] **dampening** { **dampened-paths** | **flap-statistics** | **parameters** }

show ip bgp [**vrf** *vrf-name*] **neighbors** [{ *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**advertised-routes** [**check**] | **ha-mode** [**adj-in** [**detail**] | **adj-out**] | **hide-info** | **policy** [**detail**] | **received-routes** | **routes**]]

show ip bgp [**vrf** *vrf-name*] **paths**

show ip bgp [**vrf** *vrf-name*] **summary**

show ip bgp [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**ha-mod adj-out** | **summary**]

Parameter Description

prefix-ipv4-address: IPv4 address of a specified prefix.

network-mask: Mask of a specified network prefix.

longer-prefixes: Displays the specific routing information included in a specified prefix.

aggregate: Displays the detailed information of an aggregate route.

cidr-only: Displays the classless routing information.

community: Displays the routing information that contains the specified community number.

community-number&<1-n>: Specified community attribute number. &<1-n> specifies that this parameter can be entered *n* times. This parameter follows the format of AA:NN (AS number: 2-byte number) or is set to one of the following community names:

- **gshut**
- **internet**
- **local-as**
- **no-advertise**
- **no-export**

exact-match: Specifies the routing information that exactly matches community values or a community list.

community-list *community-name*: Displays the BGP routing information that matches a specified community list. *community-name* specifies the name of a community list.

extcommunity-list *extcommunity-name*: Displays the BGP routing information that contains the name of a specified extended community list or the number of a community list. *extcommunity-name* specifies the name of an extended community list or the number of a community list.

filter-list *path-list-number*: Displays the routing information that matches the filtering list. *path-list-number* is the number of a filtering list. The value range is from 1 to 500.

global-vrf detail: Displays the global VRF information.

inconsistent-as: Displays the inconsistent routing information of the source AS.

prefix-list *ip-prefix-list-name*: Displays the routing information that matches a specified prefix filtering list.

quote-regexp *regexp*: Displays the routing information that matches a regular expression within the specified double quotation marks in the AS-PATH attribute.

regexp *regexp*: Displays the routing information that matches a specified regular expression in the AS-PATH attribute.

route-map *map-tag*: Displays the routing information that matches the filtering condition of a specified route map. *map-tag*: Name of a route map.

vrf *vrf-name*: Specifies a VRF name.

dampening: Displays the IPv4 unicast route flapping information configured by BGP.

dampened-paths: Displays the suppressed routes in the BGP IPv4 routing information.

flap-statistics: Displays the route flapping statistics in the BGP IPv4 routing information.

parameters: Displays the parameters of the IPv4 unicast route flapping information configured by BGP.

neighbors: Displays the BGP IPv4 unicast neighbor information.

neighbor-ipv4-address: IPv4 address of a specified neighbor.

neighbor-ipv6-address: IPv6 address of a specified neighbor.

advertised-routes: Displays all the routing information sent to a specified peer.

check: Displays route filtering debugging information.

ha-mode: Displays BGP NSR information.

adj-in: Displays the routing information received by the BGP neighbor NSR.

adj-out: Displays the routing information sent by the BGP neighbor NSR.

hide-info: Displays internal information.

policy: Displays the routing policy information about the BGP neighbor.

received-routes: Displays all the routing information received from a specified peer, including received routes and rejected routes.

routes: Displays all the routing information received from peers.

paths: Displays IPv4 unicast routing information in a routing information base.

summary: Displays BGP IPv4 unicast summary information.

update-group: Displays BGP IPv4 unicast update group information.

update-group-index: Specific update group information.

ha-mod adj-out: Displays the routing information sent by the BGP neighbor NSR.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The **show ip bgp** command has the same function as the **show bgp ipv4 unicast** command. All the parameters in the latter command can be used in the former command.

Examples

N/A

Notifications

N/A

Platform Description

N/A

1.186 stats-reporting-period

Function

Run the **stats-reporting-period** command to configure the interval of regularly sending state statistics by BGP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BMP does not regularly send state statistics by default.

Syntax

stats-reporting-period *report-time*

no stats-reporting-period

default stats-reporting-period

Parameter Description

report-time: Automatic scanning interval, in seconds. The value range is from 30 to 65535.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the interval of regularly sending state statistics by BGP. If the statistics count result is 0, no information is sent. If this command is not configured, each change in the statistics count causes the software to send state statistics. Frequent change in the count causes the software to send much state statistics, which wastes device resources.

Examples

The following example sets the interval of regularly sending state statistics by BMP to **30** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# stats-reporting-period 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.187 synchronization

Function

Run the **synchronization** command to enable the function of routing information synchronization between BGP and IGP.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of routing information synchronization between BGP and IGP is disabled by default.

Syntax

synchronization

no synchronization
default synchronization

Parameter Description

N/A

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

BGP and IGP synchronization aims to prevent any possible route black hole.

In the following situations, users can disable synchronization to fast converge routing information:

- No routing information passes through this local AS. Generally, this AS is a stub AS.
- All devices within the AS run BGP. A full mesh of connections is established among all BGP speakers (a neighbor relationship is established between each two BGP speakers).

Examples

The following example enables the function of routing information synchronization between BGP and IGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# synchronization
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.188 table-map

Function

Run the **table-map** command to control the routing information sent to the core routing table by BGP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

BGP does not modify the attribute of routing information sent to the core routing table by default.

Syntax

table-map *route-map-name*

no table-map

default table-map

Parameter Description

route-map-name: Name of an applied route map.

Command Modes

BGP configuration mode

Configuration mode of the IPv4 unicast/VRF address family of BGP

Configuration mode of the IPv6 unicast/VRF address family of BGP

Scope configuration mode of BGP

Default Level

14

Usage Guidelines

This command is effective to only IPv4 address families.

You can run this command to control the routing information sent to the core routing table by BGP. You can run this command to modify the attribute of routing information sent to the core routing table. If the route is matched, BGP modifies the attribute of the routing information and sends the route. If the route is not matched or route matching is denied, BGP does not modify the attribute of the routing information, but still sends the route.

Changes in the configuration of this command are not reflected in the core routing table immediately, but reflected a moment later. To update the routing table immediately, you can run the **clear ip bgp** [**vrf** *vrf-name*] **table-map** command. You run the **clear ip bgp** [**vrf** *vrf-name*] **table-map** command to not change the routes sent to the core routing table. If you run the **table-map** command, you do not result in forwarding flapping.

Examples

The following example configures BGP to filter and update routes to the core routing table based on the route map bgp_tm.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# table-map bgp_tm
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.189 timers bgp

Function

Run the **timers bgp** command to configure the duration of BGP timers.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default sending interval and hold time of Keepalive messages are **60** seconds and **180** seconds respectively. The minimum hold time is not limited.

Syntax

timers bgp *keepalive-time holetime* [*minimum-holdtime*]

no timers bgp

default timers bgp

Parameter Description

keepalive-time: Interval in seconds of sending Keepalive messages to a specified BGP peer. The value range is from 0 to 65535, and the default value is **60**.

holdtime: Valid interval in seconds of a BGP peer. The value range is from 0 to 65535, and the default value is **180**.

minimum-holdtime: Minimum hold time in seconds of a neighbor advertisement. The value range is from 0 to 65535, and the value **0** specifies no limit.

Command Modes

BGP configuration mode

Scope VRF configuration mode of BGP

Default Level

14

Usage Guidelines

The *keepalive-interval* value cannot be greater than 1/3 of the *holdtime*.

If time is configured for a single peer or peer group, this peer or peer group is connected with peers based on the configured time other than the globally configured time.

Examples

The following example sets the sending interval and hold time of Keepalive messages to **80** seconds and **240** seconds respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# timers bgp 80 240
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.190 update-source

Function

Run the **update-source** command to configure a network interface used to establish a TCP connection with a specified BMP server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The optimal local interface is used as the output interface by default.

Syntax

update-source *interface-type interface-number*

no update-source

default update-source

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

BMP configuration mode

Default Level

14

Usage Guidelines

You can run this command to establish a TCP connection with BMP servers through the loopback interface.

If you directly specify a network interface to establish a TCP connection, the address of the network interface must be a local valid one. Otherwise, the TCP connection cannot be established.

Examples

The following example uses loopback 1 interface as a TCP source address to establish a connection with the BGP peer 10.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bmp server 1
Hostname(config-bmpsrvr)# update-source loopback 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 VRF Commands

Command	Function
address-family	Enable the IPv4 or IPv6 protocol in a multiprotocol VPN Routing and Forwarding Table (VRF) and enter the corresponding address family configuration mode.
alloc-label	Configure the label allocation mode.
description	Configure the description of the VRF.
exit-address-family	Exit the address family configuration mode of the multiprotocol VRF.
export map	Configure a policy for exporting the extended community attributes of VPN routes from the local VRF to the remote device.
import map	Configure a policy for importing VPN routes from a remote device to the local VRF.
ip vrf	Configure a single-protocol VRF.
ip vrf forwarding	Add an interface to a single-protocol VRF.
ip vrf receive	Import the direct route and host route of an interface to a specified VRF.
maximum routes	Configure the maximum number of routes in a VRF.
rd	Configure the RD value of a VRF.
route-target	Configure the RT value of a VRF.
vrf definition	Configure a multiprotocol VRF.
vrf forwarding	Add an interface to a multiprotocol VRF.
vrf global-vrf	Enter the global VRF configuration mode.
vrf receive	Import the IPv4 or IPv6 local host routes and direct routes of an interface to a specified VRF.
show global-vrf	Display the global VRF information.
show ip vrf	Display the VRF information.
show vrf	Display the VRF information.

1.1 address-family

Function

Run the **address-family** command to enable the IPv4 or IPv6 protocol in a multiprotocol VPN Routing and Forwarding Table (VRF) and enter the corresponding address family configuration mode.

Run the **no** form of this command to disable the IPv4 or IPv6 protocol for the multiprotocol VRF.

Run the **default** form of this command to restore the default configuration.

No IPv4 or IPv6 protocol is enabled for the multiprotocol VRF by default.

Syntax

address-family { **ipv4** | **ipv6** }

no address-family { **ipv4** | **ipv6** }

default address-family { **ipv4** | **ipv6** }

Parameter Description

ipv4: Enables the IPv4 protocol and enters the IPv4 address family configuration mode.

ipv6: Enables the IPv6 protocol and enters the IPv6 address family configuration mode.

Command Modes

Multiprotocol VRF configuration mode

Global VRF configuration mode

Default Level

14

Usage Guidelines

This command applies to only multiprotocol VRFs.

Examples

The following example configures a multiprotocol VRF named **vrf1**, enables the IPv4 protocol, and enters the IPv4 address family configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **exit-address-family**
- **vrf definition**
- **vrf receive**

1.2 alloc-label

Function

Run the **alloc-label** command to configure the label allocation mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No label allocation mode is configured by default.

Syntax

alloc-label { **per-route** | **per-vrf** }

no alloc-label

default alloc-label

Parameter Description

per-route: Configures the label allocation mode based on each VPN route.

per- vrf: Configures the label allocation mode based on each VRF.

Command Modes

Single-protocol VRF configuration mode

Configuration mode of multiprotocol VRF IPv4 address family

Configuration mode of multiprotocol VRF IPv6 address family

Configuration mode of global VRF IPv4 address family

Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

RFC4364 describes two label allocation modes in L3VPN applications:

- Route-based label allocation mode:

  One route corresponds to one label. The advantage is that the system can look up the ILM table based on the label value and quickly forward packets to the next hop. The disadvantage is that the capacity of the ILM table must be large.

- VRF-based label allocation mode:

One VRF corresponds to one label. The advantage is that all routes in the VRF share this label, which reduces the capacity of the ILM table. The disadvantage is that packet forwarding is slower than that in route-based label allocation mode. This is because the system needs to look up the table twice in the forwarding process. It first looks up the ILM table to find the VRF where the packet is located, and then forwards the packet based on the destination IP address in the routing table of the VRF.

Examples

The following example configures the route-based label allocation mode for the single-protocol VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf VPNA
Hostname(config-vrf)# alloc-label per-route
```

The following example configures the route-based label allocation mode for the IPv4 address family of the multiprotocol VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition VPNA
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# alloc-label per-route
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **address-family**
- **vrf forwarding**

1.3 description

Function

Run the **description** command to configure the description of the VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No VRF description is configured by default.

Syntax

description *description*

Parameter Description

description: Description of a configured VRF. It is a case-sensitive string of 1 to 244 characters.

Command Modes

Single-protocol VRF configuration mode

Multiprotocol VRF configuration mode

Global VRF configuration mode

Default Level

14

Usage Guidelines

This command is applicable to both the single-protocol and multiprotocol VRFs.

Examples

The following command configures a single-protocol VRF named **vrf1** and sets its description to **vpn-a**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf vrf1
Hostname(config-vrf)# description vpn-a
```

The following command configures a multiprotocol VRF named **vrf2** and sets its description to **vpn- b** .

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf2
Hostname(config-vrf)# description vpn-b
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **vrf definition**

1.4 exit-address-family

Function

Run the **exit-address-family** command to exit the address family configuration mode of the multiprotocol VRF.

Syntax

exit-address-family

Parameter Description

N/A

Command Modes

Configuration mode of multiprotocol VRF IPv4 address family

Configuration mode of multiprotocol VRF IPv6 address family

Configuration mode of global VRF IPv4 address family

Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

N/A

Examples

The following example exits the IPv4 address family configuration mode of the multiprotocol VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# exit-address-family
Hostname(config-vrf)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **address-family**
- **vrf definition**
- **vrf receive**

1.5 export map

Function

Run the **export map** command to configure a policy for exporting the extended community attributes of VPN routes from the local VRF to the remote device.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No policy for exporting the extended community attributes associated with the VRF is configured by default.

Syntax

export map *route-map-name*

no export map

default export map

Parameter Description

map *route-map-name*: Configures the name of the associated route map.

Command Modes

Single-protocol VRF configuration mode

Configuration mode of multiprotocol VRF IPv4 address family

Configuration mode of multiprotocol VRF IPv6 address family

Configuration mode of global VRF IPv4 address family

Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

To more precisely control the extended community attributes of exported routes, you can define a precise rule as needed in the associated route map. You can run this command to add or modify the extended community attributes defined by the **route-target export** command. You can only run the **match ip address** and **set extcommunity** commands to configure rules for a route map associated by this command.

Examples

The following example configures an associated export policy for the VRF **VPNA**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf VPNA
Hostname(config-vrf)# export map rma
```

Notifications

1. When unsupported commands, such as **set ip tos**, are configured in the route map associated by this command, the following notification will be displayed:

```
% bgp export map not support set ip tos
```

2. When the associated route map such as **imp_map** does not exist, the following notification will be displayed:

```
% route-map imp_map not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **address-family**
- **vrf forwarding**

1.6 import map

Function

Run the **import map** command to configure a policy for importing VPN routes from a remote device to the local VRF.

Run the **no** form of this command to remove the import policy associated with the VRF.

Run the **default** form of this command to restore the default configuration.

No import policy associated with the VRF is configured by default.

Syntax

import map *route-map-name*

no import map

default import map

Parameter Description

map *route-map-name*: Configures the name of the associated route map.

Command Modes

Single-protocol VRF configuration mode

Configuration mode of multiprotocol VRF IPv4 address family

Configuration mode of multiprotocol VRF IPv6 address family

Configuration mode of global VRF IPv4 address family

Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

To more precisely filter routes imported to the local VRF, you can define a precise rule as needed in the associated route map. The rule defined by the **import map** command takes effect after the **Import** extended community attributes defined in the VRF. That is, only after these routes match the extended community attributes defined by the **route-target import** command in the VRF, the VPN routes received from the remote device can be filtered again by rules defined the **import map** command. You can only run the **match ip address** and **match extcommunity** commands to configure rules for a route map associated by the **import map** command.

Examples

The following example configures an import policy associated with the VRF **VPNA**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf VPNA
Hostname(config-vrf)# import map rma
```

Notifications

1. When unsupported commands, such as **set ip tos**, are configured in the route map associated by this command, the following notification will be displayed:

```
% bgp export map not support set ip tos
```

2. When the associated route map such as **exp_map** does not exist, the following notification will be displayed:

```
% route-map exp_map not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **address-family**
- **vrf forwarding**

1.7 ip vrf

Function

Run the **ip vrf** command to configure a single-protocol VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No single-protocol VRF is configured by default.

Syntax

ip vrf *vrf-name*

no ip vrf *vrf-name*

default ip vrf *vrf-name*

Parameter Description

vrf-name: Name of the single-protocol VRF. It is a case-sensitive string of 1 to 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a single-protocol VRF **redvrf**, and enters the VRF configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf redvrf
Hostname(config-vrf)#
```

The following example deletes the single-protocol VRF **redvrf**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip vrf redvrf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf forwarding**
- **ip vrf receive**
- **description**
- **show ip vrf**
- **show vrf**

1.8 ip vrf forwarding

Function

Run the **ip vrf forwarding** command to add an interface to a single-protocol VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is added to any single-protocol VRF by default.

Syntax

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

default ip vrf forwarding *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF. This VRF must be a single-protocol VRF.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

On a VRF-enabled device, if you add an interface to a single-protocol VRF and enable IPv6 on the interface, the device does not forward the IPv6 packets received on this interface. Therefore, to add an interface to a VRF and enable IPv6 on the interface, run the **vrf forwarding** command.

Examples

The following example adds the interface GigabitEthernet 0/1 to a single-protocol VRF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip vrf forwarding redvrf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**

1.9 ip vrf receive

Function

Run the **ip vrf receive** command to import the direct route and host route of an interface to a specified VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No direct route and host route of an interface are imported to any specified VRF by default.

Syntax

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

default ip vrf receive *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF. This VRF must be a single-protocol VRF.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The **ip vrf receive** command is used to select a VRF based on policy-based routing (PBR). This command imports the host route and direct route of the primary and secondary addresses of an interface to a specified VRF. To import the host route and direct route of an interface to multiple VRFs, run this command multiple times. Unlike the **ip vrf forwarding** command, this command does not add the interface to a VRF, and the interface is still global.

The **ip vrf forwarding** and **ip vrf receive** commands are mutually exclusive on a specified interface. If you configure the two commands one after another, an error prompt is displayed.

If you configure **ip vrf forwarding** and then **ip vrf receive**, the following notification will be displayed:

```
% Cannot configure 'ip vrf receive' if interface is under a VRF
```

If you configure **ip vrf receive** and then **ip vrf forwarding**, the following notification will be displayed:

```
% Cannot configure 'ip vrf forwarding VRF_1' on this interface, please unconfigure ’ip vrf receive’ and ’vrf receive’ first
```

Examples

The following example imports the host route and direct route in the network segment for the interface GigabitEthernet 0/1 to **VRF_1** and **VRF_2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip vrf receive VRF_1
Hostname(config-if-GigabitEthernet 0/1)# ip vrf receive VRF_2
Hostname(config-if-GigabitEthernet 0/1)# end
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**

1.10 maximum routes

Function

Run the **maximum routes** command to configure the maximum number of routes in a VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of routes is not configured by default.

Syntax

maximum routes *limit* { *warning-threshold* | **warning-only** }

no maximum routes

default maximum routes

Parameter Description

limit: Maximum number of routes in a VRF. Beyond this limit, no more routes are written into the core routing table. The value range is from 1 to 4294967295.

warning-threshold: Warning log threshold, in percentage. Once this threshold is reached, the warning log is displayed. The value range is from 1 to 100.

warning-only: Specifies that when the maximum number of routes is reached, warnings are displayed, but routes can still be added to the core routing table.

Command Modes

Single-protocol VRF configuration mode
Configuration mode of multiprotocol VRF IPv4 address family
Configuration mode of multiprotocol VRF IPv6 address family
Configuration mode of global VRF IPv4 address family
Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

This command is used to limit the number of routes in a VRF. To receive warnings only, specify *warning-only*.

Examples

The following example sets the maximum number of routes in the single-protocol VRF **vrf1** to 1,000, and displays warnings when the number of such routes exceeds 1,000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf vrf1
Hostname(config-vrf)# maximum routes 1000 warning-only
```

The following example sets the maximum number of routes in the single-protocol VRF **vrf2** to 10,000, and displays warnings when the number of such routes exceeds 10,000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# maximum routes 10000 warning-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**

1.11 rd

Function

Run the **rd** command to configure the RD value of a VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No RD value is configured for a VRF by default.

Syntax

rd *rd-value*

no rd

default rd

Parameter Description

rd-value: RD value of the VRF. The following RD formats are supported:

as-num: *nn*, where *as-num* is the 2-byte public AS number, and *nn* is defined by the user, and ranges from 0 to 4294967295.

Ip-addr: *nn*, where *ip-addr* must be a global IP address, and *nn* is defined by the user, and ranges from 0 to 65535.

as4-num: *nn*, where *as4-num* is a 4-byte public AS number and ranges from 1 to 4294967295 (1.0 to 65535.65535 in dot mode), and *nn* is defined by the user, and ranges from 1 to 65535.

Command Modes

Single-protocol VRF configuration mode

Multiprotocol VRF configuration mode

Global VRF configuration mode

Default Level

14

Usage Guidelines

The existing RD value of a VRF cannot be modified. To modify an existing RD value, you must first delete the VRF, reconfigure the VRF, and then configure the RD value. A VRF has only one RD value.

The RD value of the 4-byte AS is in the format of AS4:NN. AS4 can be expressed in decimal or dot mode. AS4 range is from 1 to 4294967295, which is from 1.0 to 65535.65535 in dot mode. NN ranges from 1 to 65535.

The AS number in the range of 1 to 65535 is displayed in both decimal mode and dot mode. Therefore, save the AS number in the range from 1 to 65535 as a 2-byte AS number.

Examples

The following example sets the RD value of **vrf1** to **100:1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf vrf1
Hostname(config-vrf)# rd 100:1
```

Notifications

1. If the configuration modifies an existing RD, the following error prompt will be displayed:

```
% Configuration can't be changed
```

2. If the configuration deletes an existing RD, the following error prompt will be displayed:

```
% Can not delete an exist rd value!
```

3. If the configured RD value is used by another VRF, for example, the RD of **vrf2** is set to **100:1**, the following error prompt will be displayed:

```
% "rd" 100:1 already in use by VRF vrf1
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **address-family**
- **vrf forwarding**

1.12 route-target

Function

Run the **route-target** command to configure the RT value of a VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No RT value is configured for a VRF by default.

Syntax

route-target { **both** | **export** | **import** } *route-value*

no route-target { **both** | **export** | **import** } *route-value*

default route-target { **both** | **export** | **import** } *route-value*

Parameter Description

both: Configures both the **Import** and **Export** RT attributes.

export: Configures the **Export** RT attribute.

import: Configures the **Import** RT attribute.

route-value: Value of the RT. The following RD formats are supported:

as-num: *nn*, where *as-num* is the 2-byte public AS number, and *nn* is defined by the user, and ranges from 0 to 4294967295.

Ip-addr: *nn*, where *ip-addr* must be a global IP address, and *nn* is defined by the user, and ranges from 0 to 65535.

as4-num: *nn*, where *as4-num* is a 4-byte public AS number and ranges from 1 to 4294967295 (1.0 to 65535.65535 in dot mode), and *nn* is defined by the user, and ranges from 1 to 65535.

Command Modes

Single-protocol VRF configuration mode

Multiprotocol VRF configuration mode

Configuration mode of multiprotocol VRF IPv4 address family

Configuration mode of multiprotocol VRF IPv6 address family

Global VRF configuration mode

Configuration mode of global VRF IPv4 address family

Configuration mode of global VRF IPv6 address family

Default Level

14

Usage Guidelines

You can configure multiple **Import** or **Export** RT values for a VRF.

Examples

The following example configures the RT for **vrf1**. Set the **Import** RT values to **100:1** and **100:4**, and the **Export** RT values to **100:2** and **100:4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip vrf vrf1
Hostname(config-vrf)# route-target import 100:1
Hostname(config-vrf)# route-target export 100:2
Hostname(config-vrf)# route-target both 100:4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **address-family**
- **vrf forwarding**

1.13 vrf definition

Function

Run the **vrf definition** command to configure a multiprotocol VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No multiprotocol VRF is configured by default.

Syntax

vrf definition *vrf-name*

no vrf definition *vrf-name*

default vrf definition *vrf-name*

Parameter Description

vrf name: Name of the multiprotocol VRF. It is a case-sensitive string of 1 to 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are not allowed to run the **ip vrf** command to edit a multiprotocol VRF, or run the **vrf definition** command to edit a single-protocol VRF.

Examples

The following example configures a multiprotocol VRF **vrf1**, and enters the VRF configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#vrf definition vrf1
Hostname(config-vrf)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **address-family**
- **exit-address-family**
- **vrf forwarding**
- **show vrf**

1.14 vrf forwarding

Function

Run the **vrf forwarding** command to add an interface to a multiprotocol VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is added to any multiprotocol VRF by default.

Syntax

vrf forwarding *vrf-name*

no vrf forwarding *vrf-name*

default vrf forwarding *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF. This VRF must be a multiprotocol VRF.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You are not allowed to run the **ip vrf forwarding** command to add an interface to a multiprotocol VRF, or run the **vrf forwarding** command to add an interface to a single-protocol VRF.

You are not allowed to add an interface to a multiprotocol VRF not configured with any address family.

When you add an interface to a multiprotocol VRF, existing IPv4/IPv6 or VRRP IPv4/IPv6 addresses on the interface are deleted, and the IPv6 protocol is disabled on the interface.

When you add an interface to a multiprotocol VRF not configured with any IPv4 address family, you are not allowed to configure the IPv4 and VRRP IPv4 addresses on this interface. You must configure the IPv4 address family for the multiprotocol VRF before configuring the IPv4 and VRRP IPv4 addresses on this interface.

When you add an interface to a multiprotocol VRF without any IPv6 address family, you are not allowed to configure the IPv6 and VRRP IPv6 addresses on this interface. You must configure the IPv6 address family for the multiprotocol VRF before configuring the IPv6 or VRRP IPv6 addresses on this interface.

If the IPv4 address family is deleted from the multiprotocol VRF, the IPv4 and VRRP IPv4 addresses of all interfaces added to this VRF are deleted, and the IPv4 static routes in the VRF or the IPv4 static routes with this VRF as their next-hop VRF are also deleted. If the IPv6 address family is deleted from the multiprotocol VRF, the IPv6 and VRRP IPv6 addresses of all interfaces added to the VRF are deleted. When the IPv6 protocol is disabled on the interface, the IPv6 static routes in the VRF or the IPv6 static routes with this VRF as their next-hop VRF are also deleted.

Examples

The following example adds the interface GigabitEthernet 0/1 to the multiprotocol VRF **vrf1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# exit-address-family
Hostname(config-vrf)# address-family ipv6
Hostname(config-vrf-af)# exit-address-family
Hostname(config-vrf)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# vrf forwarding vrf1
Hostname(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 1000::1/64
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **address-family**
- **exit-address-family**
- **vrf receive**

1.15 vrf global-vrf

Function

Run the **vrf global-vrf** command to enter the global VRF configuration mode.

By default, a global VRF exists, and the IPv4 and IPv6 address families are enabled for this global VRF.

Syntax

vrf global-vrf

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enters the global VRF configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf global-vrf
Hostname(config-global-vrf)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 vrf receive

Function

Run the **vrf receive** command to import the IPv4 or IPv6 local host routes and direct routes of an interface to a specified VRF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no IPv4 or IPv6 local host route and direct route of an interface are imported to a specified VRF.

Syntax

vrf receive *vrf-name*

no vrf receive *vrf-name*

default vrf receive *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF. This VRF must be a multiprotocol VRF.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command does not add the interface to the specified VRF, and the interface is still a global interface.

If you need to use PBR to select a VRF, run the **vrf receive** command on the interface to which PBR is applied to import the direct route and host route on the interface to each VRF available for choice.

When you configure the IPv4 address family for a multiprotocol VRF, the IPv4 local host route and direct route of the interface are added to the IPv4 routing table of the specified VRF, and the IPv4 local host route in the VRRP group on this interface in Master state is also added to the IPv4 routing table of the specified VRF, When you configure the IPv6 address family for a multiprotocol VRF, the IPv6 local host route and direct route of the

interface are added to the IPv6 routing table of the specified VRF, and the IPv6 local host route in Master state in the VRRP group on this interface is also added to the IPv6 routing table of the specified VRF,

On a specified interface, **ip vrf forwarding** and **vrf receive** are mutually exclusive, so are **vrf forwarding** and **vrf receive**. If you configure any of the above pairs of commands for an interface one after another, an error prompt is displayed.

If you configure **ip vrf forwarding** or **vrf forwarding** and then **vrf receive**, the following notification will be displayed:

```
% Cannot configure 'vrf receive' if interface is under a VRF
```

If you run **vrf receive**, and then **ip vrf forwarding** or **vrf forwarding**, the following notification will be displayed:

```
% Cannot configure 'vrf forwarding vrf2' on this interface, please delete'ip vrf receive' and 'vrf receive' first.
```

Examples

The following example enables the interface GigabitEthernet 0/1 to select a VRF based on IPv6 PBR.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf1
Hostname(config-vrf)# address-family ipv6
Hostname(config-vrf-af)# exit-address-family
Hostname(config-vrf)# vrf definition vrf2
Hostname(config-vrf)# address-family ipv6
Hostname(config-vrf-af)# exit-address-family
Hostname(config-route-map)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 policy route-map pbr-vrf-selection
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 1000::1/64
Hostname(config-if-GigabitEthernet 0/1)# vrf receive vrf1
Hostname(config-if-GigabitEthernet 0/1)# vrf receive vrf2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **address-family**
- **exit-address-family**
- **vrf definition**

1.17 show global-vrf

Function

Run the **show global-vrf** command to display the global VRF information.

Syntax

show global-vrf [**count** | **brief** | **detail** | **ipv4** | **ipv6**]

Parameter Description

count: Displays the VRF capacity and the current number of configured VRFs.

brief: Displays the brief information of the single-protocol and multiprotocol VRFs.

detail: Displays the detailed information of the single-protocol and multiprotocol VRFs.

ipv4: Displays the brief information of the single-protocol and multiprotocol VRFs for which the IPv4 address family is configured.

ipv6: Displays the brief information of the multiprotocol VRFs for which the IPv6 address family is configured.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the brief information of all VRFs.

```
Hostname> enable
Hostname# show global-vrf
Name                Default RD          Protocol(s)     Interface
@#global-vrf          <not set>           ipv4,ipv6      GigabitEthernet 0/1
```

Table 1-1 Output Fields of the show global-vrf Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF
Interfaces	Interface list of the VRF

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 show ip vrf

Function

Run the **show ip vrf** command to display the VRF information.

Syntax

show ip vrf [**brief** | **count** | **detail** | **interfaces**] [*vrf-name*]

Parameter Description

brief: Displays the brief information of the VRF and its interfaces.

count: Displays the VRF capacity and the current number of configured VRFs.

detail: Displays the detailed information of the VRF.

interfaces: Displays the detailed information of the interfaces to which the VRF applies.

vrf-name: Name of a configured VRF.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the information of a single-protocol VRF.

```
Hostname> enable
Hostname# show ip vrf
Name                                Interfaces
aaa                                 GigabitEthernet 0/0
                                    GigabitEthernet 0/1
```

Table 1-2 Output Fields of the show ip vrf Command

Field	Description
Name	Name of the VRF.
Interfaces	Interface list of the VRF.

The following example displays the brief information of a single-protocol VRF.

```
Hostname> enable
Hostname# show ip vrf brief
Name                          Default RD              Interfaces
refvrf                        <not set>
vrf1                          <not set>
```

Table 1-3 Output Fields of the show ip vrf brief Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF
Interfaces	Interface list of the VRF

The following example displays the VRF capacity and the current number of configured VRFs.

```
Hostname> enable
Hostname# show ip vrf count
  VRF Limit:                512
  Count of in use instances:   3
  Count of remaining instances: 509
```

Table 1-4 Output Fields of the show ip vrf count Command

Field	Description
VRF Limit	VRF capacity limit.
Count of in use instances	Number of configured VRFs.
Count of remaining instances	Number of VRFs that can be configured.

The following example displays the detailed information of a single-protocol VRF.

```
Hostname> enable
Hostname# show ip vrf detail
VRF refvrf (VRF ID = 1); default RD <not set>
  No interfaces
VRF Table ID = 1
```

```
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  Alloc-label per-vrf: -/aggregate(refvrf)
Route warning limit 1000, current count 4
```

Table 1-5 Output Fields of the show ip vrf detail Command

Field	Description
VRF	Name of the VRF
VRF ID	VRF ID associated with the VRF name
default RD	Default RD of the VRF
VRF Table ID	ID of the VRF table.
Export VPN route-target communities	VPN RT community attributes to be exported
Import VPN route-target communities	VPN RT community attributes to be imported.
import route-map	Route map information to be imported
export route-map	Route map information to be exported
Alloc-label per-vrf	Label value allocated to each VRF

The following example displays the interface information of a VRF.

```
Hostname> enable
Hostname# show ip vrf interfaces
Interface           IP-Address      VRF          Protocol
```

Table 1-6 Output Fields of the show ip vrf interface Command

Field	Description
Interface	Interface list of the VRF.
IP-Address	IP address of the interface
VRF	Name of the VRF
Protocol	Protocol ID

Notifications

N/A

Platform Description

N/A

Related Commands

- ip vrf

1.19 show vrf

Function

Run the **show vrf** command to display the VRF information.

Syntax

show vrf [**brief** | **count** | **detail** | **ipv4** | **ipv6**] [*vrf-name*]

Parameter Description

brief: Displays the brief information of VRFs.

count: Displays the VRF capacity and the current number of configured VRFs.

detail: Displays the detailed information of VRFs.

ipv4: Displays the information of VRFs configured with an IPv4 address family.

ipv6: Displays the information of VRFs configured with an IPv6 address family.

vrf-name: Specifies the name of the VRF to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to display single-protocol and multiprotocol VRFs.

Examples

The following example displays all VRFs.

```
Hostname> enable
Hostname# show vrf
  Name       Default RD        Protocols   Interfaces
  aaa        <not set>         ipv4
  aab        <not set>
  bbb        <not set>         ipv6
  ccc        <not set>         ipv4,ipv6   Vl1
```

Table 1-7 Output Fields of the show vrf Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF

Protocol	Address family enabled for the VRF. ● **IPv4** indicates that the IPv4 address family is enabled. ● **IPv6** Indicates that the IPv6 address family is enabled.
Interfaces	Interface list under the VRF, that is, the list of interfaces configured with the **vrf forwarding** or **ip vrf forwarding** command.

The following example displays the information of VRFs for which the IPv4 address family is configured.

```
Hostname> enable
Hostname# show vrf ipv4
Name               Default RD          Protocol(s)         Interface
refvrf             <not set>           ipv4               <none>
vrf1               <not set>           ipv4               <none>
```

Table 1-8 Output Fields of the show vrf ipv4 Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF
Protocol	Address family enabled for the VRF ● **IPv4** indicates that the IPv4 address family is enabled. ● **IPv6** Indicates that the IPv6 address family is enabled.
Interfaces	Interface list under the VRF, that is, the list of interfaces for which the **vrf forwarding** or **ip vrf forwarding** command is configured.

The following example displays the information of VRFs for which the IPv6 address family is configured.

```
Hostname> enable
Hostname# show vrf ipv6
Name              Default RD              Protocol(s)     Interface
mvrf              <not set>               ipv6           <none>
```

Table 1-9 Output Fields of the show vrf ipv6 Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF
Protocol	Address family enabled for the VRF ● **IPv4** indicates that the IPv4 address family is enabled. ● **IPv6** Indicates that the IPv6 address family is enabled.

Interfaces	Interface list under the VRF, that is, the list of interfaces for which the **vrf forwarding** or **ip vrf forwarding** command is configured.

The following example displays the brief information of a VRF.

```
Hostname> enable
Hostname# show vrf brief
Name               Default RD              Protocol(s)     Interface
mvrf               <not set>               ipv6           <none>
refvrf              <not set>               ipv4           <none>
```

Table 1-10 Output Fields of the show vrf brief Command

Field	Description
Name	Name of the VRF
Default RD	Default RD of the VRF
Protocol	Address family enabled for the VRF ● **IPv4** indicates that the IPv4 address family is enabled. ● **IPv6** Indicates that the IPv6 address family is enabled.
Interfaces	Interface list under the VRF, that is, the list of interfaces for which the **vrf forwarding** or **ip vrf forwarding** command is configured.

The following example displays the VRF capacity and the current number of configured VRFs.

```
Hostname> enable
Hostname# show vrf count
VRF Limit:                512
  Count of in use instances:   3
  Count of remaining instances: 509
```

Table 1-11 Output Fields of the show vrf count Command

Field	Description
VRF Limit	VRF capacity limit
Count of in use instances	Number of configured VRFs
Count of remaining instances	Number of VRFs that can be configured

The following example displays the detailed information of a VRF.

```
Hostname> enable
Hostname# show vrf detail
VRF mvrf (VRF ID = 4); default RD <not set>; default VPNID <not set>
```

```
  No interfaces
Address family ipv4 not active.
Address family ipv6:
  No import route-map
  No export route-map
  Alloc-label per-vrf: -/aggregate(mvrf)

VRF refvrf (VRF ID = 1); default RD <not set>
  No interfaces
VRF Table ID = 1
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  Alloc-label per-vrf: -/aggregate(refvrf)
Route warning limit 1000, current count 4
```

Table 1-12 Output Fields of the show vrf detail Command

Field	Description
VRF	Name of the VRF
default RD	Default RD of the VRF
default VPNID	Default VPN ID of the VRF
Address family ipv4	Information of the configured IPv4 address family
Address family ipv6	Information of the configured IPv6 address family
import route-map	Route map information to be imported
export route-map	Route map information to be exported
Export VPN route-target communities	VPN RT community attributes to be exported
Import VPN route-target communities	VPN RT community attributes to be imported
Alloc-label per-vrf	Label value allocated to each VRF

Notifications

N/A

Platform Description

N/A

Related Commands

- **ip vrf**
- **vrf definition**

1 Routing Policy Commands

Command	Function
ip as-path access-list	Configure an autonomous system (AS) path filtering rule based on a regular expression.
ip community-list	Configure a community list.
ip extcommunity-list	Configure an extcommunity list to be used by a route map. This route map is used to filter virtual private network (VPN) routes in the BGP application. **standard** defines a standard community list and controls access to this list. **expanded** defines an expanded community list and controls access to this list. After an extcommunity list is created, the system enters the **ip extcommunity-list** configuration mode.
ip prefix-list	Create a prefix list or add a prefix list entry.
ip prefix-list description	Add a text description for a prefix list.
ip prefix-list sequence-number	Enable the function of displaying sequence numbers in a prefix list.
ipv6 prefix-list	Create an IPv6 prefix list or add a prefix list entry.
ipv6 prefix-list description	Add a text description for an IPv6 prefix list.
ipv6 prefix-list sequence-number	Enable the function of displaying sequence numbers in an IPv6 prefix list.
match as-path	Configure the AS path attribute permitted in the ACL to match routes.
match community	Configure the community attribute permitted in the ACL to match routes.
match extcommunity	Configure an extcommunity list to match routes.
match interface	Configure a specified interface as the next-hop outbound interface.
match ip address	Configure the target network routes that are permitted in an ACL or prefix list.
match ip next-hop	Configure the target network routes whose next-hop IP addresses match rules in the ACL or prefix list.

match ip policy	Configure the target network routes that are permitted in the ACL and match a specified L3 authentication traffic diversion domain type.
match ip route-source	Configure the target network routes whose source IP addresses match rules in the ACL or prefix list.
match ipv6 address	Configure the target IPv6 network routes that are permitted in the ACL or prefix list.
match ipv6 next-hop	Configure the target network routes whose next-hop IPv6 addresses match rules in the ACL or prefix list.
match ipv6 route-source	Configure the target network routes whose source IPv6 addresses match rules in the ACL or prefix list.
match metric	Configure the metric values of routes.
match origin	Configure the source type of BGP routes.
match route-type	Configure the route type.
match tag	Configure the tags of routes.
memory-lack exit-policy	Specify the exit policy for the upper-layer routing protocols when the free memory space reaches the lower level.
route-map	Configure a route map and enter the route map configuration mode.
set aggregator as	Specify the AS value of the aggregator for routes that match the rules.
set aigp-metric	Specify the Accumulated IGP Metric Attribute (AIGP) metric for routes that match the rules.
set as-path replace	Replace the AS_PATH values for routes that match the rules with specified values.
set as-path prepend	Add the specified AS_PATH values for routes that match the rules.
set atomic-aggregate	Configure the atomic-aggregate attribute for routes.
set comm-list delete	Delete all community values from routes that match the rules according to the community list.
set community	Specify the community values for routes that match the rules.
set dampening	Configure the flapping parameters for routes that match the rules.

set distance	Configure the management distance for routes that match the rules.
set extcomm-list delete	Delete all extended community values from the routes that match the rules according to the extcommunity list.
set extcommunity	Specify the extended community values for routes that match the rules.
set fast-reroute	Specify the backup outbound interface and backup next hop of FRR for routes that match the rules.
set ip default next-hop	Specify the default next-hop IPv4 address for packets that match the rules.
set ip dscp	Configure the differentiated service code point (DSCP) value for packets matching the rules.
set ip next-hop	Specify the next-hop IPv4 address for packets that match the rules.
set ip next-hop recursive	Specify the recursive next-hop IP address for packets that match the rules.
set ip next-hop self	Set the next hop to the device itself for packets that match the rules.
set ip next-hop unchanged	Set the next hops of routes that match the rules to keep unchanged.
set ip next-hop verify-availability	Verify availability of the next-hop IPv4 address.
set ip precedence	Configure the priority of the IPv4 header for packets that match the rules.
set ip tos	Configure the ToS of the IPv4 header for a packet that matches the rules.
set ipv6 default next-hop	Specify the default next-hop IPv6 address for IPv6 packets that match the rules.
set ipv6 next-hop	Specify the next-hop IPv6 address for IPv6 packets that match the rules.
set ipv6 next-hop recursive	Specify the recursive next-hop IPv6 address for packets that match the rules.
set ipv6 next-hop self	Set the next hop to the device itself for IPv6 routes that match the rules.

set ipv6 next-hop unchanged	Set the next hop to keep unchanged for IPv6 routes that match the rules.
set ipv6 next-hop verify-availability	Verify availability of the next-hop IPv6 address.
set ipv6 precedence	Configure the priority of the IPv6 header for packets that match the rules.
set l3vpn nexthop local-vrf	Set the L3 VPN next hop to the local VRF instance for packets matching the match rules.
set level	Specify the type of the destination area to which routes that match the rules will be advertised.
set local-preference	Configure the LOCAL_PREFERENCE value for routes that match the rules.
set metric	Configure the metric value for routes that match the rules.
set metric-type	Configure the metric type for routes that match the rules.
set next-hop	Specify the next-hop IP address for routes that match the rules.
set next-hop self	Set the next hop to the device itself for routes that match the rules.
set next-hop unchanged	Set the next hop to keep unchanged for routes that match the rules.
set origin	Specify the source for routes that match the rules.
set originator-id	Specify the originator address for routes that match the rules.
set qos-id	Specify the QoS ID for routes that match the rules.
set tag	Configure the tag for routes that match the rules.
set weight	Configure the weight for BGP routes that match the rules.
show ip as-path-access-list	Display the AS-path list information.
show ip community-list	Display the community list information.
show ip extcommunity-list	Display the extcommunity list information.
show ip prefix-list	Display the information about a prefix list or prefix list entries.

show ip protocols	Display the status information of the IPv4 routing protocols that are currently running.
show ipv6 prefix-list	Display the information about an IPv6 prefix list or prefix list entries.
show route-map	Display the route map configurations.

1.1 ip as-path access-list

Function

Run the **ip as-path access-list** command to configure an autonomous system (AS) path filtering rule based on a regular expression.

Run the **no** form of this command to remove this configuration.

By default, no AS path filtering rule is configured.

Syntax

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

no ip as-path access-list *path-list-num* [{ **permit** | **deny** } *regular-expression*]

Parameter Description

path-list-num: Identifier of an AS path list. The value range is from 1 to 500.

permit: Permits access.

deny: Denies access.

regular-expression: Regular expression. It is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an AS path filtering rule to match only the path information containing the AS number of 123.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip as-path access-list 105 deny ^123$
```

Notifications

When you delete an AS path filtering rule, if the entered rule name or the filtering rule does not exist, the following notification will be displayed:

```
% This object doesn't exist
```

If you enter an invalid filtering rule, the following notification will be displayed:

```
% Can't compile regexp
```

When you configure a duplicate AS path filtering rule, the following notification will be displayed:

```
% Insertion failed with duplicate policy
```

Common Errors

N/A

Platform Description

N/A

Related Commands

show ip bgp filter-list (BGP)

1.2 ip community-list

Function

Run the **ip community-list** command to configure a community list.

Run the **no** form of this command to remove this configuration.

By default, no community list is configured.

Syntax

ip community-list { *community-list-number* | **standard** *community-list-name* } { **permit** | **deny** } [{ *community-list-number* | **internet** | **local-AS** | **no-advertise** | **no-export** | **gshut** }]

ip community-list { *community-list-number* | **expanded** *community-list-name* } { **permit** | **deny** } [*regular-expression*]

no ip community-list { { **standard** | **expanded** } *community-list-name* | *community-list-number* }

Parameter Description

standard: Specifies a standard community list.

expanded: Specifies an expanded community list.

community-list-name: Name of a community list. It is a string of less than 80 characters.

community-list-number: Number of a community list. For a standard community list, the range is from 1 to 99. For an expanded community list, the range is from 100 to 199.

permit: Permits access.

deny: Denies access.

community-number: Value of the community attribute. The format is AA:NN (AS number: 2-byte number) or the value is a number. The value range is from 0 to 4294967295.

Internet: Specifies the Internet community. All paths belong to this community.

local-AS: Specifies that the path matching a route in the community list is not advertised to other ASs. When an AS alliance is configured, the path is not advertised to other ASs or sub ASs.

no-advertise: Specifies that the path is not advertised to any Border Gateway Protocol (BGP) peer.

no-export: Specifies that the path is not advertised to External Border Gateway Protocol (EBGP) peers.

gshut: Specifies that the route matching the community list is advertised by a graceful shutdown neighbor.

regular-expression: Regular expression. It is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to define a community list used for BGP. **standard** defines a standard community list and controls access to this list. **expanded** defines an expanded community list and controls access to this list.

A community list supports up to 32 community values, including **internet**, **local-AS**, **no-advertise**, and **no-export**.

Examples

The following example configures the standard community list **test** to reject routes that contain the community attributes of **100:20** and **200:20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip community-list standard test deny 100:20 200:20
```

The following example configures the standard community list **test2** to allow routes that contain the community attribute of **Internet**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip community-list standard test2 permit internet
```

Notifications

If the name of a specified community list is all numbers, the following notification will be displayed:

```
% Community-list name cannot have all digits
```

If the name of a specified community list contains more than 80 characters, the following notification will be displayed:

```
% Community-list name lengths should be less than 80 chars
```

When you delete a community list but the entered list or filtering rule does not exist, the following notification will be displayed:

```
% This object doesn't exist
```

When you configure a duplicate community filtering rule, the following notification will be displayed:

```
% Insertion failed with duplicate policy
```

When you configure a community filtering rule with a duplicate sequence number, the following notification will be displayed:

```
% Community-list entry with this sequence already exist
```

When you configure both a standard community list and an expanded community list by using the same name, the following notification will be displayed:

```
% Community-list name conflict with previous defined
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip extcommunity-list

Function

Run the **ip extcommunity-list** command to configure an extcommunity list to be used by a route map. This route map is used to filter virtual private network (VPN) routes in the BGP application. **standard** defines a standard community list and controls access to this list. **expanded** defines an expanded community list and controls access to this list. After an extcommunity list is created, the system enters the **ip extcommunity-list** configuration mode.

Run the **no** form of this command to remove this configuration.

By default, no extcommunity list is configured.

Syntax

ip extcommunity-list { *standard-list* | **standard** *list-name* } { **permit** | **deny** } [**rt** *rt-value* | **soo** *soo-value*]

ip extcommunity-list { *expanded-list* | **expanded** *list-name* } { **permit** | **deny** } [*regular-expression*]

ip extcommunity-list { *expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* }

no ip extcommunity-list { *expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* }

Parameter Description

expand-list: ID of an expanded extcommunity list. The value range is from 100 to 199. One extcommunity list may contain multiple rules.

standard-list: ID of a standard extcommunity list. The value range is from 1 to 99. One extcommunity list may contain multiple rules.

expanded *list-name*: Specifies the name of an expanded extcommunity list. When this parameter is used, the system enters the expanded extcommunity list configuration mode. The name contains up to 32 characters.

standard *list-name*: Specifies the name of a standard extcommunity list. When this parameter is used, the system enters the standard extcommunity list configuration mode. The name contains up to 32 characters.

permit: Defines a permit extcommunity rule.

deny: Defines a deny extcommunity rule.

regular-expression: Regular expression used to define a template for matching an extcommunity. It is a string of 1 to 255 characters.

rt *rt-value* | **soo** *soo-value*: Configures the extcommunity attributes to be matched. You can enter the route target (RT) and site of origin (SOO) attributes for multiple times.

rt *rt-value*: Configures the RT attribute. This parameter can be used only for the standard extcommunity configuration, but not for the expanded extcommunity configuration.

soo *soo-value*: Configures the SOO attribute. This parameter can be used only for the standard extcommunity configuration, but not for the expanded extcommunity configuration.

rt-value and *soo-value*: Value of an extended community (extend_community_value).

extend_community_value has three options:

extend_community _value = as_num:nn

as_num is a 2-byte public AS number. nn is configurable. The value range is from 0 to 4294967295.

extend_community_value = ip_addr:nn

ip_addr must be a global IP address. nn is configurable. The value range is from 0 to 65535.

extend_community_value = as4_num:nn

an4_num is a 4-byte public AS number. nn is configurable. The value range is from 1 to 65535. The AS number range is from 1 to 4294967295, or 1 to 65535.65535 in dot mode.

Command Modes

Global configuration mode and ip extcommunity-list configuration mode

Default Level

14

Usage Guidelines

This command is used to create an extcommunity list that has multiple extcommunity values. This list is used in the **match extcommunity** rule in a route map to match the extcommunity attribute of BGP routes, so as to achieve the purpose of route filtering.

In the definition of an expanded extcommunity rule, *regular-expression* is described as follows:

- Character: No special meaning.
- Period (.): Matches any single character.
- Asterisk (*): Matches zero or any sequence in a string.
- Plus sign (+): Matches one or any sequence in a string.
- Question mark (?): Matches zero or one symbol in a string.
- Caret (^): Matches the start of a string.
- Dollar sign ($): Matches the end of a string.
- Underline (_): Matches commas, brackets, start and end of a string, and spaces.
- Square brackets ([]): Matches a single character within a range.

In expanded ip extcommunity-list configuration mode, the following commands are available:

- [*sequence-number*] **deny** *regular-expression*: Defines a deny extcommunity rule.
- [*sequence-number*] **permit** *regular-expression*: Defines a permit extcommunity rule.
- **exit:** Exits the current mode.
- **no** [*sequence-number*] **deny** *regular-expression*: Deletes a deny extcommunity rule.
- **no** [*sequence-number*] **permit** *regular-expression*: Deletes a permit extcommunity rule.

In standard ip extcommunity-list configuration modes, the following commands are available:

- [*sequence-number*] **deny** { [**rt** *value*] [**soo** *value*] }: Defines a deny extcommunity rule.
- [*sequence-number*] **permit** { [**rt** *value*] [**soo** *value*] }: Defines a permit extcommunity rule.
- **exit**: Exits the current mode.
- **no** [*sequence-number*] **deny** { [**rt** *value*] [**soo** *value*] }: Deletes a deny extcommunity rule.
- **no** [*sequence-number*] **permit** { [**rt** *value*] [**soo** *value*] }: Deletes a permit extcommunity rule.

Examples

The following example configures the extcommunity list **1** to allow traffic with the RT attribute of 100:1.

The following example configures the standard extcommunity list **aaa** to allow traffic with the RT attribute of 100:2.

The following example configures the expanded extcommunity list **ext1** to allow traffic with the extcommunity attribute of 200:[0~9][0~9].

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip extcommunity-list 1 permit rt 100:1
Hostname(config)# ip extcommunity-list standard aaa permit rt
100:2
Hostname(config)# ip extcommunity-list expanded ext1 permit 200:[0~9][0~9]
```

The following example configures the route map **rt_in_filter** to match routes with the extcommunity lists **1** and **ext1**, and applies the route map to the VPN address family in AS 65000 of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map rt_in_filter
Hostname(config-route-map)# match extcommunity 1
Hostname(config-route-map)# match extcommunity ext1
Hostname(config)# router bgp 65000
Hostname(config-router)# address-family vpn
Hostname(config-router-af)# neighbor 3.3.3.3 send-community extended
Hostname(config-router-af)# neighbor 3.3.3.3 route-map rt_in_filter in
```

Notifications

When you delete a community list but the entered list or filtering rule does not exist, the following notification will be displayed:

```
% This object doesn't exist
```

When you configure a duplicate extcommunity filtering rule, the following notification will be displayed:

```
% Insertion failed with duplicate policy
```

When you configure an extcommunity filtering rule with a duplicate sequence number, the following notification will be displayed:

```
% Extcommunity-List entry with this sequence already exist
```

When you configure both a standard and expanded extcommunity lists with the same name, the following notification will be displayed:

```
% Extcommunity-list name conflict with previous defined
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip prefix-list

Function

Run the **ip prefix-list** command to create a prefix list or add a prefix list entry.

Run the **no** form of this command to remove this configuration.

By default, no prefix list is configured.

Syntax

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

Parameter Description

prefix-list-name: Name of a prefix list.

seq-number: Sequence number assigned to a prefix list entry. The value range is from 1 to 2147483647. If no sequence number is specified in this command, the system will assign a default sequence number to the prefix list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each unassigned entry is the first multiple of 5 and greater than the previous sequence number.

deny: Denies access when rules are matched.

permit: Permits access when rules are matched.

ipv4-prefix: Network address and mask. The mask length ranges from 0 to 32.

minimum-prefix-length: Minimum range (namely, the start length of a range).

maximum-prefix-length: Maximum range (namely, the end length of a range).

Note

- The keyword **ge** indicates the greater than or equal to operation.
- The keyword **le** indicates the smaller than or equal to operation.
- If both **ge** and **le** are not configured, rules are matched only when the mask length is exactly the same as the configured mask length.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **ip prefix-list** command is used to configure an IP prefix list. The keyword **permit** or **deny** in a prefix list determines the permit or deny action when the prefix list is matched.

The prefix list defines the exact match or range match for a prefix. The keyword **ge** or **le** defines the prefix range used for matching, and provides more flexible matching configuration than *ipv4-prefix*. If the keyword **ge** or **le** is not configured in the command, *ipv4-prefix* provides an accurate prefix range for matching. If only **ge** is configured, the matching range is from *minimum-prefix-length* to 32. If only **le** is configured, the matching range is from *ipv4-prefix* to *maximum-prefix-length*. If both are configured, the matching range is from *minimum-prefix-length* to *maximum-prefix-length*. That is, the relationship between *ipv4-prefix* mask length, *minimum-prefix-length*, and *maximum-prefix-length* is as follows: *ipv4-prefix* mask length < *minimum-prefix-length* < *maximum-prefix-length* <= 32.

Examples

The following example configures the prefix list **pre1** to match the traffic with the address segment 201.1.1.0/24, and filters the routing information output when RIP routes are redistributed to OSPF based on **pre1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip prefix-list pre1 permit 201.1.1.0/24
Hostname(config)# router ospf
Hostname(config-router)# distribute-list prefix pre1 out rip
Hostname(config-router)# end
```

Notifications

When you configure a prefix list entry with duplicate rules, the following notification will be displayed:

```
% Insertion failed with duplicate policy
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip prefix-list description

Function

Run the **ip prefix-list description** command to add a text description for a prefix list.

Run the **no** form of this command to remove this configuration.

By default, no text description is configured for a prefix list.

Syntax

ip prefix-list *prefix-list-name* **description** *description-text*

no ip prefix-list *prefix-list-name* **description**

Parameter Description

prefix-list-name: Name of a prefix list.

description-text: Text description of a prefix list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example adds the text description "Deny routes from Net-A" for the prefix list **pre**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip prefix-list pre description Deny routes from Net-A
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip prefix-list sequence-number

Function

Run the **ip prefix-list sequence-number** command to enable the function of displaying sequence numbers in a prefix list.

Run the **no** form of this command to disable this feature.

By default, the function of displaying sequence numbers in a prefix list is disabled.

Syntax

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of displaying sequence numbers in a prefix list.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip prefix-list sequence-number
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ipv6 prefix-list

Function

Run the **ipv6 prefix-list** command to create an IPv6 prefix list or add a prefix list entry.

Run the **no** form of this command to remove this configuration.

By default, no prefix list is configured.

Syntax

ipv6 prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

no ipv6 prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix- length*] [**le** *maximum-prefix-length*]

Parameter Description

prefix-list-name: Name of a prefix list.

seq-number: Sequence number assigned to a prefix list entry. The value range is from 1 to 2147483647. If no sequence number is specified in this command, the system will assign a default sequence number to the prefix list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each entry not assigned a value is the first multiple of 5 greater than the previous sequence number.

deny: Denies access when rules are matched.

permit: Permits access when rules are matched.

ipv6-prefix: Network address and mask. The mask value range is from 0 to 128.

minimum-prefix-length: Minimum range (namely, the start length of a range).

maximum-prefix-length: Maximum range (namely, the end length of a range).

Note

- The keyword **ge** indicates the greater than or equal to operation.
- The keyword **le** indicates the smaller than or equal to operation.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **ipv6 prefix-list** command is used to configure an IPv6 prefix list. The keyword **permit** or **deny** in a prefix list determines the permit or deny action when the prefix list is matched.

The prefix list defines the exact match or range match for a prefix. The keyword **ge** or **le** defines the prefix range used for matching, and provides more flexible matching configuration than *ipv6-prefix*. If the keyword **ge** or **le** is not configured in the command, *ipv6-prefix* provides an accurate prefix range for matching. If only **ge** is configured, the matching range is from *minimum-prefix-length* to 128. If only **le** is configured, the matching range is from *ipv6-prefix* to *maximum-prefix-length*. If both are configured, the matching range is from *minimum-prefix-length* to *maximum-prefix-length*. That is, the relationship between *ipv6-prefix* mask length, *minimum-prefix-length*, and *maximum-prefix-length* is as follows: *ipv6-prefix* mask length < *minimum-prefix-length* < *maximum-prefix-length* <= 128.

Examples

The following example configures the IPv6 prefix list **pre** to allow traffic in the address segment 2222::/64, and filters the routing information output when the OSPF process **1** is redistributed to RIP based the IPv6 prefix list **pre**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 prefix-list pre permit 2222::/64
Hostname(config)# ipv6 router rip
Hostname(config-router)# redistribute ospf 1
Hostname(config-router)# distribute-list prefix pre out
Hostname(config-router)# end
```

Notifications

When you configure an IPv6 prefix list entry with duplicate rules, the following notification will be displayed:

```
% Insertion failed with duplicate policy
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ipv6 prefix-list description

Function

Run the **ipv6 prefix-list description** command to add a text description for an IPv6 prefix list.

Run the **no** form of this command to remove this configuration.

By default, no text description is configured for a prefix list.

Syntax

ipv6 prefix-list *prefix-list-name* **description** *description-text*

no ipv6 prefix-list *prefix-list-name* **description**

Parameter Description

prefix-list-name: Name of an IPv6 prefix list.

description-text: Text description of an IPv6 prefix list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example adds the text description "Deny routes from Net-A" for the IPv6 prefix list **pre**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ipv6 prefix-list sequence-number

Function

Run the **ipv6 prefix-list sequence-number** command to enable the function of displaying sequence numbers in an IPv6 prefix list.

Run the **no** form of this command to disable this feature.

By default, the function of displaying sequence numbers in a prefix list is disabled.

Syntax

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of displaying sequence numbers in an IPv6 prefix list.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 prefix-list sequence-number
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 match as-path

Function

Run the **match as-path** command to configure the AS path attribute permitted in the ACL to match routes.

Run the **no** form of this command to remove this configuration.

By default, no AS-path list is configured for packet matching.

Syntax

match as-path *as-path-acl-list-number*&<1-10>

no match as-path *as-path-acl-list-number*&<1-10>

Parameter Description

as-path-acl-list-number&<1-10>: Number of an ACL. The value range is from 1 to 500. &<1-10> indicates that you can enter the parameters up to 10 times in this command.

By default, if you do not specify the ACL number when removing the ACL configurations, all ACLs are removed.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

When using this command in BGP, you can configure multiple ACL numbers in this command.

In a route map policy, one or more **match** or **set** commands can be configured. If no **match** command is configured, all traffic is matched. If no **set** command is configured, no operation is performed.

Examples

The following example configures the route map **ROUTEMAP2IBGP**, and matches routes with the AS-path lists **20** and **30**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# route-map ROUTEMAP2IBGP
Hostname(config-route-map)# match as-path 20 30
```

Notifications

If more than 10 AS-path lists are configured, the following notification will be displayed:

```
% Match as-path command only support 10 aspath-access-list
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 match community

Function

Run the **match community** command to configure the community attribute permitted in the ACL to match routes.

Run the **no** form of this command to remove this configuration.

By default, no community list is configured.

Syntax

match community { *community-list-number* | *community-list-name* } [**exact-match** | *community-list-number* | *community-list-name*]&<1-6>

no match community { *community-list-number* | *community-list-name* } [**exact-match** | *community-list-number* | *community-list-name*]&<1-6>

Parameter Description

[**exact-match** | *community-list-number* | *community-list-name*]&<1-6>: &<1-6> indicates that you can enter the parameters up to six times in this command.

community-list-number: Number of a community list. For a standard community list, the range is from 1 to 99. For an extcommunity list, the range is from 100 to 199.

community-list-name: Name of a community list. It is a string of less than 80 characters.

exact-match: Specifies the exact match list.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

When using this command in BGP, you can configure up to six community list numbers or names in total in this command. Every **exact-match** keyword applies only to the previous list, instead of all lists.

In a route map rule, one or more **match** or **set** commands can be configured. If no **match** command is configured, all rules are matched. If no **set** command is configured, no operation is performed.

Examples

The following example configures the community list **1** to allow traffic with the community values of 100:2 and 100:30, and configures the route map **set_lopref** to set the local preference to 20 for routes that exactly match the community list **1** in the route map.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip community-list 1 permit 100:2 100:30
Hostname(config)# route-map set_lopref
Hostname(config-route-map)# match community 1 exact-match
Hostname(config-route-map)# set local-preference 20
```

Notifications

If the name of a specified community list of the name type is all numbers, the following notification will be displayed:

```
% Community-list name cannot have all digits
```

If the name of a specified community list contains 80 characters or more, the following notification will be displayed:

```
% Community-list name lengths should be less than 80 chars
```

If more than six community lists are configured in a single command, the following notification will be displayed:

```
% Match community command only support six community-list
```

If more than six community lists are configured in total, the following notification will be displayed:

```
% Match community can't exceed 6!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 match extcommunity

Function

Run the **match extcommunity** command to configure an extcommunity list to match routes.

Run the **no** form of this command to remove this configuration.

By default, no extcommunity list is configured.

Syntax

match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }&<1-6>

no match extcommunity [*standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name*]&<1-6>

Parameter Description

{ *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }&<1-6>: &<1-6> indicates that you can enter the parameters up to six times in this command.

standard-list-number: Number of a standard extcommunity list. The value range is from 1 to 99.

standard-list-name: Name of a standard extcommunity list.

expanded-list-num: Number of an expanded extcommunity list. The value range is from 100 to 199.

expanded-list-name: Name of an expanded extcommunity list.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

When using this command in BGP, you can configure multiple extcommunity list numbers or names in this command but ensure that the total count does not exceed six. An extcommunity list may contain multiple extcommunity attribute values.

A route map that uses the extcommunity attributes for matching is applicable to the following scenarios:

- In the route map associated with the **import map** command, the RT attribute is used to filter routes imported to the virtual routing and forwarding (VRF) instance.
- In the route map associated with the **neighbor route-map in** and **neighbor route-map out** commands, if the **match extcommunity** command is configured in VPNv4 address family configuration mode of BGP, the RT attribute is used to filter VPNv4 routes that are received from or will be sent to a BGP peer.

Examples

The following example configures the extcommunity list **1** to allow traffic with the RT values of 100:1 and 100:2.

```
Hostname(config)# ip extcommunity-list 1 permit rt 100:1
Hostname(config)# ip extcommunity-list 1 permit rt 100:2
```

The following example defines a match rule in route map configuration mode.

```
Hostname(config)# route-map rt
Hostname(config-route-map)# match extcommunity 1
```

The following example applies the route map to the VPNV4 address family in BGP 100.

```
Hostname(config)# router bgp 100
Hostname(config-router)# address-family vpnv4
```

```
Hostname(config-router-af)# neighbor 3.3.3.3 route-map rt in
```

Notifications

If the name of a specified extcommunity list of the name type is all numbers, the following notification will be displayed:

```
% Extcommunity-list name cannot have all digits
```

If the name of a specified extcommunity list name contains 80 characters or more, the following notification will be displayed:

```
% Extcommunity-list name lengths should be less than 80 chars
```

If more than six extcommunity lists are configured in a single command, the following notification will be displayed:

```
% Match extcommunity command only support six extcommunity-list
```

If more than six extcommunity lists are configured in total, the following notification will be displayed:

```
% Match extcommunity can't exceed 6!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 match interface

Function

Run the **match interface** command to configure a specified interface as the next-hop outbound interface.

Run the **no** form of this command to remove this configuration.

By default, no next-hop outbound interface is configured.

Syntax

match interface { *interface-type interface-number* }&<1-4>

no match interface [*interface-type interface-number*]&<1-4>

Parameter Description

interface-type: Interface type.

interface-number: Interface number.

{ *interface-type interface-number* }&<1-4>: &<1-4> indicates that you can enter the parameters up to four times in this command.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

You can configure multiple interfaces in this command.

Note

By default, if you do not specify the interface type or number when removing the configurations, the configurations of all interfaces are removed.

Examples

The following example configures the route map **redrip** to match traffic with the GigabitEthernet 0/1 interface that is used as the outbound interface, and filters RIP routes redistributed to OSPF based on the rule in the route map **redrip**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match interface GigabitEthernet 0/1
```

Notifications

If more than four interface are specified, the following notification will be displayed:

```
% Match interface can't exceed 4!
```

If the specified interface is an L2 interface (for example, L2 interface GigabitEthernet 0/0), the following notification will be displayed:

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 match ip address

Function

Run the **match ip address** command to configure the target network routes that are permitted in an ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no ACL or prefix list used for packet matching is configured.

Syntax

match ip address { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

no match ip address [[*acl-number* | *acl-name*]&<1-6> | **prefix-list** *prefix-list-name*&<1-6>]

Parameter Description

acl-number: Number of an ACL. The following value ranges are supported. For a standard IP ACL, the range is from 1 to 99 or from 1300 to 1999. For an extended IP ACL, the range is from 100 to 199 or from 2000 to 2699.

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*&<1-6>: Specifies the name of the prefix list to be matched. &<1-6> indicates that you can enter the parameters up to six times in this command.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

You can configure multiple ACL numbers or names in this command.

Note

By default, if you do not specify the ACL number when removing the ACL configurations, configurations of all ACLs are removed.

Examples

The following example configures a route map to redistribute only RIP routes that match the ACL 10 to OSPF, and sets the route type to the external route type-1 and the initial metric to 40.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# access-list 10 permit 200.168.23.0 0.0.0.255
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ip address 10
Hostname(config-route-map)# set metric 40
Hostname(config-route-map)# set metric-type type-1
```

Notifications

If the specified ACL name is invalid, for example, **match ip address 12345**, the following notification will be displayed:

```
% ACL name 12345 is invalid
```

If you configure this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you configure this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

If more than six ACLs are specified in a single command, the following notification will be displayed:

```
% Match ip address command only support six IP access-list
```

If more than six ACLs are configured in total, the following notification will be displayed:

```
% ACL can't exceed 6!
```

If more than six prefix lists are specified in a single command, the following notification will be displayed:

```
% Match ip address command only support six IP prefix-list
```

If more than six prefix lists are configured in total, the following notification will be displayed:

```
% Prefix-list can't exceed 6!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 match ip next-hop

Function

Run the **match ip next-hop** command to configure the target network routes whose next-hop IP addresses match rules in the ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no ACL or prefix list used for next-hop IP address matching is configured.

Syntax

match ip next-hop { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

no match ip next-hop [[*acl-number* | *acl-name*]&<1-6> | **prefix-list** *prefix-list-name*&<1-6>]

Parameter Description

acl-number: Number of an ACL. The following value ranges are supported. For a standard IP ACL, the range is from 1 to 99 or from 1300 to 1999. For an extended IP ACL, the range is from 100 to 199 or from 2000 to 2699.

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*&<1-6>: Specifies the name of the prefix list to be matched. &<1-6> indicates that you can enter the parameters up to six times in this command.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

You can configure multiple ACL numbers or names in this command.

Note

By default, if you do not specify the ACL number when removing the ACL configurations, configurations of all ACLs are removed.

Examples

The following example configures the route map **redrip** to match traffic with the next-hop IP addresses matching ACL 10 or 20, and redistributes RIP routes to OSPF based on the rule in the route map **redrip**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# access-list 10 permit host 192.168.10.1
Hostname(config)# access-list 20 permit host 172.16.20.1
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ip next-hop 10 20
```

Notifications

If the specified ACL name is invalid, for example, **match ip next-hop 12345**, the following notification will be displayed:

```
% ACL name 12345 is invalid
```

If you use this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you use this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

If more than six ACLs are specified in a single command, the following notification will be displayed:

```
% Match ip next-hop command only support six IP access-list
```

If more than six ACLs are configured in total, the following notification will be displayed:

```
% ACL can't exceed 6!
```

If more than six prefix lists are specified in a single command, the following notification will be displayed:

```
% Match ip next-hop command only support six IP prefix-list
```

If more than six prefix lists are configured in total, the following notification will be displayed:

```
% Prefix-list can't exceed 6!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 match ip policy

Function

Run the **match ip policy** command to configure the target network routes that are permitted in the ACL and match a specified L3 authentication traffic diversion domain type.

Run the **no** form of this command to remove this configuration.

Syntax

match ip policy { *acl-number* | *acl-name* }&<1-6> **class** *class-id*

no match ip policy [*acl-number* | *acl-name*]&<1-6>

Parameter Description

acl-number: Number of an ACL. The following value ranges are supported. For a standard IP ACL, the range is from 1 to 99 or from 1300 to 1999. For an extended IP ACL, the range is from 100 to 199 or from 2000 to 2699.

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

class-id: ID of the L3 authentication traffic diversion domain type. The value range is from 1 to 60. The L3 authentication traffic diversion domain type is specified by the Web authentication module.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for policy-based routing (PBR) configuration.

You can configure only one ACL number or name in this command. *class-id* indicates the L3 authentication traffic diversion domain type to be matched. They together describe the packets that match the specific user type.

Examples

The following example configures the route map **pbr1** to match traffic with the L3 authentication traffic diversion domain of **acl1** and set class ID of the domain type to **10**, and applies the route map **pbr1** to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip policy route-map pbr1
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# route-map pbr1 permit 10
Hostname(config-route-map)# match ip policy acl1 class 10
```

Notifications

If the specified ACL name is invalid, for example, **match ip address 12345**, the following notification will be displayed:

```
% ACL name 12345 is invalid
```

If more than one **match ip policy** is configured, the following notification will be displayed:

```
% Match ip policy command only support one rule
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 match ip route-source

Function

Run the **match ip route-source** command to configure the target network routes whose source IP addresses match rules in the ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no ACL or prefix list is configured to match the source IP addresses of routes.

Syntax

match ip route-source { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

no match ip route-source [[*acl-number* | *acl-name*]&<1-6> | **prefix-list** *prefix-list-name*&<1-6>]

Parameter Description

acl-number: Number of an ACL. The following value ranges are supported. For a standard IP ACL, the range is from 1 to 99 or from 1300 to 1999. For an extended IP ACL, the range is from 100 to 199 or from 2000 to 2699.

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*&<1-6>: Specifies the name of the prefix list to be matched. &<1-6> indicates that you can enter the parameters up to six times in this command.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

You can configure multiple ACL numbers in this command.

Note

By default, if you do not specify the ACL number when removing the ACL configurations, configurations of all ACLs are removed.

Examples

The following example configures the route map **redrip** to match traffic with the source IP addresses matching ACL 5, and redistribute RIP routes that match the rule in the route map **redrip** to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets
Hostname(config-router)# route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# access-list 5 permit host 192.168.100.1
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ip route-source 5
```

Notifications

If the specified ACL name is invalid, for example, **match ip route-source 12345**, the following notification will be displayed:

```
% ACL name 12345 is invalid
```

If you configure this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you configure this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

If more than six ACLs are specified in a single command, the following notification will be displayed:

```
% Match ip route-source command only support six IP access-list
```

If more than six ACLs are configured in total, the following notification will be displayed:

```
% ACL can't exceed 6!
```

If more than six prefix lists are specified in a single command, the following notification will be displayed:

```
% Match ip route-source command only support six IP prefix-list
```

If more than six prefix lists are configured in total, the following notification will be displayed:

```
% Prefix-list can't exceed 6!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 match ipv6 address

Function

Run the **match ipv6 address** command to configure the target IPv6 network routes that are permitted in the ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no IPv6 ACL or IPv6 prefix list is configured for packet matching.

Syntax

match ipv6 address { *acl-name* | **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*: Specifies the name of an IPv6 prefix list used for matching.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

- The sequence number of a route map can be followed by only one IPv6 ACL.
- The default sequence number of a route map is 10.
- The IPv6 PBR function cannot be used together with the parameter **prefix-list**. If they are used together, this parameter does not take effect.

Examples

The following example configures the route map **redip** to match traffic with the IPv6 ACL **v6acl** and set the metric to **30**, and applies the route map **redip** when RIP routes are redistributed to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# exit
Hostname(config)# ipv6 access-list v6acl
Hostname(config-ipv6-acl)# permit ipv6 2620::/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ipv6 address v6acl
Hostname(config-route-map)# set metric 30
```

Notifications

If the specified ACL name is invalid, for example, **match ipv6 address 123456**, the following notification will be displayed:

```
% ACL name 123456 is invalid
```

If you configure this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you configure this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 match ipv6 next-hop

Function

Run the **match ipv6 next-hop** command to configure the target network routes whose next-hop IPv6 addresses match rules in the ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no IPv6 ACL or IPv6 prefix list is configured for next-hop IP address matching.

Syntax

match ipv6 next-hop { *acl-name* | **prefix-list** *prefix-list-name* }

no match ipv6 next-hop

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*: Specifies the name of an IPv6 prefix list to be matched.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **redip** to match routes with the next hop matching the IPv6 ACL **v6acl** and set the metric to **40**, and applies the route map **redip** when RIP routes are redistributed to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# exit
Hostname(config)# ipv6 access-list v6acl
Hostname(config-ipv6-acl)# 10 permit ipv6 2720::/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ipv6 next-hop v6acl
Hostname(config-route-map)# set metric 40
```

Notifications

If the specified ACL name is invalid, for example, **match ipv6 next-hop 123456**, the following notification will be displayed:

```
% ACL name 123456 is invalid
```

If you configure this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you configure this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 match ipv6 route-source

Function

Run the **match ipv6 route-source** command to configure the target network routes whose source IPv6 addresses match rules in the ACL or prefix list.

Run the **no** form of this command to remove this configuration.

By default, no IPv6 ACL or IPv6 prefix list is configured to match the source IP addresses of routes.

Syntax

match ipv6 route-source { *acl-name* | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*: Specifies the name of an IPv6 prefix list to be matched.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **redip** to match traffic with the source IP addresses matching the IPv6 ACL **v6acl** and set the metric to **50**, and applies the route map **redip** when RIP routes are redistributed to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# exit
Hostname(config)# ipv6 access-list v6acl
Hostname(config-ipv6-acl)# 10 permit ipv6 5200::/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ipv6 route-source v6acl
Hostname(config-route-map)# set metric 50
```

Notifications

If the specified ACL name is invalid, for example, **match ipv6 route-source 123456**, the following notification will be displayed:

```
% ACL name 123456 is invalid
```

If you configure this command to configure an ACL after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set access-list match with prefix-list exits!
```

If you configure this command to configure a prefix list after you have configured a prefix list by using this command, the following notification will be displayed:

```
% Can't set prefix-list match with access-list exists!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 match metric

Function

Run the **match metric** command to configure the metric values of routes.

Run the **no** form of this command to remove this configuration.

By default, no metric values of routes are configured.

Syntax

match metric *metric*

no match metric

Parameter Description

metric: Value of the metric. The value range is from 0 to 4294967295.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **redist-rip** to match traffic with the metric value of **10**, and configures OSPF to redistribute RIP routes based on the route map **redist-rip**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redist-rip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redist-rip permit 10
Hostname(config-route-map)# match metric 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 match origin

Function

Run the **match origin** command to configure the source type of BGP routes.

Run the **no** form of this command to remove this configuration.

By default, no source type of BGP routes is configured.

Syntax

match origin { **egp** | **igp** | **incomplete** }

no match origin [**egp** | **igp** | **incomplete**]

Parameter Description

egp: Specifies that the source is the remote Exterior Gateway Protocol (EGP).

igp: Specifies that the source is the local Interior Gateway Protocol (IGP).

incomplete: Specifies that the source is incomplete.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

Only routes with a single type of source can be matched. Routes with different source types cannot be matched simultaneously.

This command is used to set the route source for matching.

Examples

The following example configures the route map **MY_MAP** to match routes with the source **egp** and sets the community to **109**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map MY_MAP 10 permit
Hostname(config-route-map)# match origin egp
Hostname(config-route-map)# set community 109
Hostname(config-route-map)# exit
```

The following example configures the route map **MAP20** to match routes with the source **incomplete** and sets the community to **no-export**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map MAP20 20 permit
Hostname(config-route-map)# match origin incomplete
Hostname(config-route-map)# set community no-export
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 match route-type

Function

Run the **match route-type** command to configure the route type.

Run the **no** form of this command to remove this configuration.

By default, no rule is configured to match any route type.

Syntax

match route-type { **static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **nssa-external** [**type-1** | **type-2**] | **level-1** | **level-2** | **evpn-type-1** | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5** }&<1-6>

no match route-type [**static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **nssa-external** [**type-1** | **type-2**] | **level-1** | **level-2** | **evpn-type-1** | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5**]&<1-n>

Parameter Description

[**static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **nssa-external** [**type-1** | **type-2**] | **level-1** | **level-2** | **evpn-type-1** | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5**]&<1-16>: &<1-16> indicates that you can enter the parameters up to 16 times in this command, with only once for each route type.

static: Specifies a static route.

connect: Specifies a direct route.

rip: Specifies an RIP route.

local: Specifies a local route.

internal: Specifies an OSPF internal route.

external: Specifies an external route (BGP or OSPF external route).

nssa-external: Specifies an OSPF NSSA external route.

type-1 | **type-2**: Specifies a type-1 or type-2 external route of OSPF.

level-1 | **level-2**: Specifies a level-1 or level-2 route of ISIS.

evpn-type-1 | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5**: Specifies the five route types of BGP EVPN.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **redrip** to match traffic with the route type **internal**, and applies the route map **redip** when OSPF routes are redistributed to RIP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# redistribute ospf route-map redrip
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match route-type internal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 match tag

Function

Run the **match tag** command to configure the tags of routes.

Run the **no** form of this command to remove this configuration.

By default, no routes with tags are matched.

Syntax

match tag *tag*&<1-4>

no match tag [*tag*&<1-4>]

Parameter Description

tag: Tag value of a route. The value range is from 0 to 4294967295. & <1-4> indicates that up to four tags can be configured.

By default, if you do not specify the optional parameter when removing the configurations, all route tag configurations are removed.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **redrip** to match routes with tags 50 and 80, and applies the route map **redip** when OSPF routes are redistributed to RIP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router rip
Hostname(config-router)# redistribute ospf 100 route-map redrip
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match tag 50 80
```

Notifications

If more than four tags are configured in total, the following notification will be displayed:

```
% Match tag can't exceed 4!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 memory-lack exit-policy

Function

Run the **memory-lack exit-policy** command to specify the exit policy for the upper-layer routing protocols when the free memory space reaches the lower level.

Run the **no** form of this command to restore the default configuration.

By default, the routing protocol with the highest memory usage exits.

Syntax

memory-lack exit-policy { **bgp** | **ospf** | **pim-sm** | **rip** }

no memory-lack exit-policy

Parameter Description

bgp: Specifies that BGP exits first when the memory is insufficient.

ospf: Specifies that OSPF exits first when the memory is insufficient.

pim-sm: Specifies that PIM-SM exits first when the memory is insufficient.

rip: Specifies that RIP exits first when the memory is insufficient.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the free memory space reaches the lower level, this command can disable one routing protocol to release the memory resources and protect the operation of other protocols in the system.

You should know routing protocols that support the main network services, and in the case of insufficient memory, disable one of the least important protocols to protect main services in this extreme situation. If you set a disabled routing protocol to exit first when the memory is sufficient, the system still cannot obtain sufficient memory resources.

Specifying a routing protocol to exit first can, to some extent, protect main network services when the system memory is insufficient. If the memory is further consumed, all routing protocols need to exit and stop running.

Examples

The following example configures a policy that enables BGP to exit first.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# memory-lack exit-policy bgp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 route-map

Function

Run the **route-map** command to configure a route map and enter the route map configuration mode.

Run the **no** form of this command to remove this configuration.

By default, no route map is configured.

Syntax

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [{ **permit** | **deny** } *sequence-number*]

Parameter Description

route-map-name: Name of a route map. You can define a name that is easy to remember. With this name, you can use the route map in the redistribution configuration commands in the routing process. Multiple policies can be defined in a route map, and one policy corresponds to one sequence number.

permit: If the **permit** keyword is defined, and the rule defined in **match** is matched, the **set** command controls route redistribution. For PBR, the **set** command controls packet forwarding and exit of the route map.

If the **permit** keyword is defined, but the rule defined in **match** is not matched, the system switches to the next route map policy until the **set** command is executed.

deny: If the **deny** keyword is defined, and the rule defined in **match** is matched, no operation is performed. This route map policy does not allow route redistribution or PBR, and the system exits the route map.

If the **deny** keyword is defined, but the rule defined in **match** is not matched, the system switches to the next route map policy until the **set** command is executed.

sequence-number: Sequence number of a route map policy. A policy with a smaller sequence number is used first. The value range is from 0 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The route map is currently used for:

- Route redistribution control

  Route redistribution control redistributes routes from one routing process to another. For example, the routes in the OSPF routing domain can be redistributed and then advertised to the RIP routing domain, or vice versa. Mutual redistribution of routes can be carried out among all IP routing protocols.

  In route redistribution, mutual distribution of routes between two routing domains is often controlled conditionally through the application of a route map. In a route map policy, one or more **match** and **set** commands can be configured. If no **match** command is configured, all traffic is matched. If no **set** command is configured, no operation is performed.

- PBR

  The PBR provides a data packet routing and forwarding mechanism that is more flexible than target network-based routing. After PBR is applied on a device, the device determines how to process packets that need to be routed according to a route map. The route map determines the next hop forwarding device of a packet.

  To apply PBR, you must specify a route map for PBR, and create this map. A route map consists of multiple policies, and one or more match rules and relevant actions are defined for each policy. After PBR is applied

to an interface, all packets received by the interface are checked. Packets that do not match any policy in the route map are routed and forwarded as usual. Packets that match a policy in the route map are processed based on the action defined in the policy.

When configuring a route map, use the sequence number of the route map as follows:

- If you do not specify *sequence-number* when creating the first route map policy, the default sequence number is 10.
- If only one route map policy exists and you do not specify *sequence-number*, a new route map policy is not created. Instead, the existing route map policy is configured.
- If multiple route map policies exist, you must specify *sequence-number*; otherwise, an error prompt is displayed.

Examples

The following example configures the route map **redrip** to match traffic with the metric value of 4, set the initial metric value to **40**, the route type to the external route **type-1**, and the route tag to **40**, and applies the route map **redip** when RIP routes are redistributed in OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match metric 4
Hostname(config-route-map)# set metric 40
Hostname(config-route-map)# set metric-type type-1
Hostname(config-route-map)# set tag 40
```

Notifications

If the specified route map name contains more than 32 characters, the following notification will be displayed:

```
% Route-map name string length can not exceed 32.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 set aggregator as

Function

Run the **set aggregator as** command to specify the AS value of the aggregator for routes that match the rules.

Run the **no** of this command to remove this configuration.

By default, no aggregator AS value is specified.

Syntax

set aggregator as *as-number ipv4-address*

no set aggregator as [*as-number ipv4-address*]

Parameter Description

as-number: AS number of the aggregator. The AS number range is from 1 to 4294967295, or 1.0 to 65535.65535 in dot mode.

ipv4-address: Address of the aggregator.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration in BGP to set the aggregator attributes of routes.

This command has only one set of parameters: *as-number* and *ipv4-address*, and does not support multiple sets of parameters.

Examples

The following example configures the route map **set-as-path** to set the AS number of the route aggregator to **3** and IP address to **2.2.2.2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map set-as-path
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set aggregator as 3 2.2.2.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 set aigp-metric

Function

Run the **set aigp-metric** command to specify the Accumulated IGP Metric Attribute (AIGP) metric for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no AIGP metric attribute is configured for routes.

Syntax

set aigp-metric { *metric-number* | **igp-metric** }

no set aigp-metric

Parameter Description

metric-number: AIGP metric value. The value range is from 0 to 4294967295.

igp-metric: Configures the AIGP metric to the IGP metric type.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration in EGP to configure the AIGP metric of routes.

This command has only one set of parameters, and does not support multiple sets of parameters.

Examples

The following example configures the route map **test** to set the AIGP metric of routes to **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map test
Hostname(config-route-map)# set aigp-metric 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 set as-path replace

Function

Run the **set as-path replace** command to replace the AS_PATH values for routes that match the rules with specified values.

Run the **no** form of this command to remove this configuration.

By default, the AS_PATH values of matched routes will not be replaced.

Syntax

set as-path replace *as-number*&<1-10>

no set as-path replace

Parameter Description

as-number&<1-10>: AS number of the AS_PATH value to be replaced. &<1-10> indicates that you can enter the parameter up to 10 times in this command.

Note

The AS number range is from 1 to 4294967295, or 1.0 to 65535.65535 in dot mode.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration to replace the AS_PATH values of matched routes. Up to 10 AS_PATH values can be replaced at a time.

Examples

The following example configures the route map **set-as-path** to replace the AS_PATH values with "100 101 102" for routes that match the AS-path list 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map set-as-path
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set as-path replace 100 101 102
```

Notifications

If more than 10 AS_PATH values are configured in total, the following notification will be displayed:

```
% Cannot have more than 10 as-paths replaced
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 set as-path prepend

Function

Run the **set as-path prepend** command to add the specified AS_PATH values for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no rule is configured to add AS_PATH values for routes.

Syntax

set as-path prepend *as-number*&<1-10>

no set as-path prepend

Parameter Description

as-number&<1-10>: AS number of the AS_PATH to be added. &<1-10> indicates that you can enter the parameter up to 10 times in this command. The AS number range is from 1 to 4294967295, or 1.0 to 65535.65535 in dot mode.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration to add the AS_PATH values to the matched routes. Up to 10 AS_PATH values can be added at a time.

Examples

The following example configures the route map **set-as-path** to add the AS_PATH values "100 101 102" for routes that match the AS-path list 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map set-as-path
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set as-path prepend 100 101 102
```

Notifications

If more than 10 AS_PATH values are configured in total, the following notification will be displayed:

```
% Cannot have more than 10 as-paths prepended
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 set atomic-aggregate

Function

Run the **set atomic-aggregate** command to configure the atomic-aggregate attribute for routes.

Run the **no** form of this command to remove this configuration.

By default, no atomic-aggregate attribute is configured for routes.

Syntax

set atomic-aggregate

no set atomic-aggregate

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used in BGP to configure the atomic-aggregate attribute for routes.

Examples

The following example configures the route map **test** to configure the atomic-aggregate attribute for routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map test
Hostname(config-route-map)# set atomic-aggregate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 set comm-list delete

Function

Run the **set comm-list delete** command to delete all community values from routes that match the rules according to the community list.

Run the **no** form of this command to remove this configuration.

By default, no community value is deleted from matched routes according to the community list.

Syntax

set comm-list { *community-list-number* | *community-list-name* } **delete**

no set comm-list { *community-list-number* | *community-list-name* } **delete**

Parameter Description

community-list-number: Number of the community list. For a standard community list, the range is from 1 to 99. For an expanded community list, the range is from 100 to 199.

community-list-name: Name of a community list, comprising less than 80 characters.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration to delete the community values from matched routes.

Examples

The following example configures the route map **ROUTEMAPIN** to delete the community values (100:10 and 100:2) from matched routes according to Community-List 500, configures the route map **ROUTEMAPOUT** to delete the community values (not 100:50 or 100:.*) from matched routes according to Community-List 120,

applies the route map **ROUTEMAPIN** to the inbound direction of the neighbor 172.16.233.33 in AS 100 of BGP,

and applies the route map **ROUTEMAPOUT** to the outbound direction of the neighbor 172.16.233.33 in AS 100 of BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 100
Hostname(config-router)# neighbor 172.16.233.33 remote-as 120
Hostname(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
```

```
Hostname(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
Hostname(config-router)# exit
Hostname(config)# ip community-list 500 permit 100:10
Hostname(config)# ip community-list 500 permit 100:20
Hostname(config)# ip community-list 120 deny 100:50
Hostname(config)# ip community-list 120 permit 100:.*
Hostname(config)# route-map ROUTEMAPIN permit 10
Hostname(config-route-map)# set comm-list 500 delete
Hostname(config-route-map)# exit
Hostname(config)# route-map ROUTEMAPOUT permit 10
Hostname(config-route-map)# set comm-list 120 delete
```

Notifications

If the name of a specified community list of the name type is all numbers, the following notification will be displayed:

```
% Community-list name cannot have all digits
```

If the name of a specified community list contains 80 characters or more, the following notification will be displayed:

```
% Community-list name lengths should be less than 80 chars
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 set community

Function

Run the **set community** command to specify the community values for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no community value is specified for a route.

Syntax

set community { **none** | { *community-number* | **internet** | **local-AS** | **no-advertise** | **no-export** }&<1-32> [**additive**] }

no set community

Parameter Description

{ *community-number* | **internet** | **local-AS** | **no-advertise** | **no-export** }&<1-32>: &<1-32> indicates that you can enter the parameter up to 32 times in this command.

community-number: Value of the community attribute.

The format is AA:NN (AS number: 2-byte number) or the value is a number. The value range is from 0 to 4294967295.

Internet: Specifies the Internet community. All paths belong to this community.

local-as: Specifies that a path is not advertised to other ASs. When an AS alliance is configured, the path is not advertised to other ASs or sub ASs.

no-advertise: Specifies that the path is not advertised to any BGP peer.

no-export: Specifies that the path is not advertised to EBGP peers.

additive: Adds a community value based on the original community attribute.

none: Keeps the community attribute empty.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the community attribute for matched routes.

Examples

The following example configures the route map **SET_COMMUNITY**, sets the community attribute to **109:10** for routes that match as-path 1 in a policy with the sequence number of 10, and sets the community attribute to **no-export** for routes that match as-path 2 in a policy with the sequence number of 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map SET_COMMUNITY 10 permit
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set community 109:10
Hostname(config-route-map)# exit
Hostname(config)# route-map SET_COMMUNITY 20 permit
Hostname(config-route-map)# match as-path 2
Hostname(config-route-map)# set community no-export
```

Notifications

If more than 32 community values are configured, the following notification will be displayed:

```
% Cannot have more than 32 community attributes
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 set dampening

Function

Run the **set dampening** command to configure the flapping parameters for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, when the half-life period is 15 minutes, and the penalty value of a route is lower than 750, route suppression is canceled. When the penalty value of a route exceeds 2000, the route is suppressed. A route can be suppressed for a maximum of 60 minutes.

Syntax

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Parameter Description

half-life: Half-life period when a route is accessible or not accessible, in minutes. The value range is from 1 to 45.

reuse: When the penalty value of a route is smaller than this value, route suppression is canceled. The value range is from 1 to 20000.

suppress: When the penalty value of a route is greater than this value, the route is suppressed. The value range is from 1 to 20000.

max-suppress-time: Longest time that a route can be suppressed, in minutes. The value range is from 1 to 255.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the flapping parameters for matched routes.

Examples

The following example configures a route map to set the route flapping parameters (*half-life*: **30** min, *reuse*: **1500**, *suppress*: **10000**, and *max-suppress-time*: **120** min), and applies the route map to BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map tag
Hostname(config-route-map)# match as path 10
Hostname(config-route-map)# set dampening 30 1500 10000 120
Hostname(config-route-map)# exit
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 172.16.233.52 route-map tag in
```

Notifications

If the configured *suppress* is smaller than *reuse* or the configured *max-suppress-time* is smaller than *half-life*, the following notification will be displayed:

```
% Invalid value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 set distance

Function

Run the **set distance** command to configure the management distance for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no management distance is modified for matched routes.

Syntax

set distance *distance-number*

no set distance

Parameter Description

distance-number: Route management distance. The value range is from 1 to 255.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

The route management distance affects route selection. Therefore, configure it carefully based on the actual network topology.

Examples

The following example configures the route map **test** to set the management distance of routes that match the rules to **112**, and applies the route map to the OSPF process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map test
Hostname(config-route-map)# set distance 112
```

```
Hostname(config)#exit
Hostname(config)# router ospf 1
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# distance 111 route-map test
Hostname(config-router)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 set extcomm-list delete

Function

Run the **set extcomm-list delete** command to delete all extended community values from the routes that match the rules according to the extcommunity list.

Run the **no** form of this command to remove this configuration.

By default, the extended community values of matched routes are not deleted.

Syntax

set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

no set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

Parameter Description

extcommunity-list-number: Number of an extcommunity list. For a standard extcommunity list, the range is from 1 to 99. For an expanded extcommunity list, the range is from 100 to 199.

extcommunity-list-name: Name of an extcommunity list. It is a string of less than 80 characters.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration to delete the extended community values from matched routes.

Examples

The following example configures the route map **ROUTEMAPIN** to delete all extended community values from routes that match the rules according to the extcommunity list 10.

The following example configures the route map **ROUTEMAPOUT** to delete all extended community values from routes that match the rules according to the extcommunity list 120.

The following example applies the route maps **ROUTEMAPIN** and **ROUTEMAPOUT** to AS 65000 in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 65000
Hostname(config-router)# neighbor 172.16.233.33 remote-as 65531
Hostname(config-router)# address-family vpnv4 unicast
Hostname(config-router-af)# neighbor 172.16.233.33 activate
Hostname(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
Hostname(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
Hostname(config-router)# exit
Hostname(config)# ip extcommunity-list 10 permit rt 100:10
Hostname(config)# ip extcommunity-list 10 permit rt 100:20
Hostname(config)# ip extcommunity-list 120 deny 100:50
Hostname(config)# ip extcommunity-list 120 permit 100:.*
Hostname(config)# route-map ROUTEMAPIN permit 10
Hostname(config-route-map)# set extcomm-list 10 delete
Hostname(config-route-map)# exit
Hostname(config)# route-map ROUTEMAPOUT permit 10
Hostname(config-route-map)# set extcomm-list 120 delete
```

Notifications

If the name of a specified extcommunity list of the name type is all numbers, the following notification will be displayed:

```
% Extcommunity-list name cannot have all digits
```

If the specified extcommunity list name contains 80 characters or more, the following notification will be displayed:

```
% Extcommunity-list name lengths should be less than 80 chars
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 set extcommunity

Function

Run the **set extcommunity** command to specify the extended community values for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no extended community values are specified for matched routes.

Syntax

set extcommunity { **rt** *extend-community-value* | **soo** *extend-community-value* }

no set extcommunity { **rt** | **soo** }

Parameter Description

rt: Configures the RT value of a route.

soo: Configures the SOO value of a route.

extend-community-value: Value of an extended community.

extend_community_value has three options:

extend_community _value = as_num:nn

as_num is a 2-byte public AS number. nn is configurable. The value range is from 0 to 4294967295.

extend_community_value = ip_addr:nn

ip_addr must be a global IP address. nn is configurable. The value range is from 0 to 65535.

extend_community_value = as4_num:nn

an4_num is a 4-byte public AS number. nn is configurable. The value range is from 0 to 65535.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration to configure the extended community values for matched routes.

Note

- You can configure the AS4 extended community, that is, the extended community with the 4-byte AS number. The format of the AS4 extended community is AS4:NN. AS4 can be expressed in decimal or dot mode. AS4 ranges from 1 to 4294967295, which is 1 to 65535.65535 in dot mode. The NN range is from 0 to 65535.
- The AS number in the range of 1 to 65535 is displayed the same in both decimal mode and dot mode. Therefore, save the AS number in the range of 1 to 65535 as a 2-byte AS number.

Examples

The following example configures the route map **MAP_NAME**, matches routes with ACL 2, and sets the extended community attribute RT to 100:2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Hostname(config)# route-map MAP_NAME permit 10
Hostname(config-route-map)# match ip address 2
Hostname(config-route-map)# set extcommunity rt 100:2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 set fast-reroute

Function

Run the **set fast-reroute** command to specify the backup outbound interface and backup next hop of FRR for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no backup outbound interface and backup next hop of FRR are specified for matched routes.

Syntax

set fast-reroute backup-interface *interface-type interface-number* **backup-nexthop** *ipv4-address*

no set fast-reroute

Parameter Description

interface-type interface-number: Backup outbound interface.

ipv4-address: Backup next hop, which is mandatory for non-P2P interfaces.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used in FRR configuration to configure the backup outbound interface and backup next hop of IP FRR. If the current software version supports only one backup route, only one set of <interface, next hop> parameters can be configured in this command.

Note

FRR backup entries should not be the direct or local host routes.

Examples

The following example configures the route map **frr** to set the backup outbound interface to **GigabitEthernet 0/1** and the backup next hop to **192.168.1.2** for routes matching ACL 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Hostname(config)# route-map frr permit 10
Hostname(config-route-map)# match ipv4-address 2
Hostname(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1
backup-nexthop 192.168.1.2
```

Notifications

If the specified interface is an L2 interface (for example, L2 interface GigabitEthernet 0/0), the following notification will be displayed:

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 set ip default next-hop

Function

Run the **set ip default next-hop** command to specify the default next-hop IPv4 address for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no default next-hop IPv4 address is specified for matched routes.

Syntax

set ip default next-hop { *ipv4-address* [*weight*] }&<1-32>

no set ip default next-hop [*ipv4-address* [*weight*]&<1-32>

Parameter Description

{ *ipv4-address* [*weight*] }&<1-32>: &<1-32> indicates that you can enter the parameter up to 32 times in this command.

ipv4-address: IP address of the next hop.

weight: Weight of the next hop.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command supports two operation modes: weighted cost multipath (WCMP) load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system performs WCMP load balancing on traffic based on the configured *weight*.

You can configure up to 32 IP addresses in this command.

If you add the *weight* value after *ipv4 address*, you can configure up to four **next-hop** addresses.

If **vrf** *vrf-name* is specified, packets are forwarded across VRF instances. If **global** is specified, packets are forwarded from the VRF instance to the public network. If [**vrf** *vrf-name* | **global**] is not specified, the VRF instance is inherited, that is, the next hop belongs to the VRF instance that receives the packets.

Note

If you configure *weight* after any **next-hop**, the operation mode of this **set** command automatically switches to WCMP load balancing mode. In WCMP load balancing mode, the default value of *weight* is **1** if *weight* is not specified for the **next-hop** address.

The difference between the **set ip next-hop** and **set ip default next-hop** commands is as follows: If the **set ip next-hop** command is configured, the system uses PBR first to forward packets. If the **set ip default next-hop** command is configured, the system uses the route forwarding table first to forward packets.

You can run this command to configure a customized default route for specific users. If the software cannot find a route to forward packets, these packets are forwarded to the next hop configured in this command.

Examples

The following example configures the route map **equal-access** to forward packets that are received by GigabitEthernet 0/1 from 1.1.1.1 to 6.6.6.6 if the software cannot find a forwarding route for them, to forward packets that are received from 2.2.2.2 to 7.7.7.7 if the software cannot find a forwarding route for them, and to drop other packets if the software cannot find a forwarding route for them.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#access-list 1 permit 1.1.1.1 0.0.0.0
Hostname(config)#access-list 2 permit 2.2.2.2 0.0.0.0
```

```
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip policy route-map equal-access
Hostname(config)#route-map equal-access permit 10
Hostname(config- route-map)#match ip address 1
Hostname(config-route-map)#set ip default next-hop 6.6.6.6
Hostname(config)#route-map equal-access permit 20
Hostname(config-route-map)#match ip address 2
Hostname(config-route-map)#set ip default next-hop 7.7.7.7
Hostname(config)#route-map equal-access permit 30
Hostname(config- route-map)#set default interface null 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 set ip dscp

Function

Run the **set ip dscp** command to configure the differentiated service code point (DSCP) value for packets matching the rules.

Run the **no** form of this command to remove this configuration.

By default, no DSCP is configured in an IPv4 packet for matched routes.

Syntax

set ip dscp *dscp_value*

no set ip dscp

Parameter Description

dscp_value: DSCP value in the IP header of an IP packet.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **smallpak** to set the DSCP value to **20** for packets that are received by GigabitEthernet 0/1 and smaller than 500 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip policy route-map smallpak
Hostname(config)# route-map smallpak permit 10
Hostname(config-route-map)# match length 0 500
Hostname(config-route-map)# set ip dscp 20
```

Notifications

If you configure this command after the **set ip tos** or **set ip precedence** command has been configured, the following notification will be displayed:

```
% Route-map: can not set ip dscp.
% Remove set ip tos/precedence clause before set ip dscp.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 set ip next-hop

Function

Run the **set ip next-hop** command to specify the next-hop IPv4 address for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no next-hop IPv4 address is specified for matched packets.

Syntax

set ip next-hop { *ipv4-address* [*weight*] }&<1-32>

no set ip next-hop [*ipv4-address* [*weight*]&<1-32>

Parameter Description

{ *ipv4-address* [*weight*] }&<1-32>: &<1-32> indicates that you can enter the parameter up to 32 times in this command.

ipv4-address: IP address of the next hop.

weight: Weight of the next hop. The value range is from 1 to 8.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration.

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system performs WCMP load balancing on traffic based on the configured weight.

You can configure up to 32 IP addresses in this command.

If you add the *weight* value after *ipv4 address*, you can configure up to four **next-hop** addresses.

If **vrf** *vrf-name* is specified, packets are forwarded across VRF instances. If **global** is specified, packets are forwarded from the VRF instance to the public network. If [**vrf** *vrf-name* | **global**] is not specified, the VRF instance is inherited, that is, the next hop belongs to the VRF instance that receives the packets.

Note

If you configure *weight* after any **next-hop**, the operation mode of this **set** command automatically switches to WCMP load balancing mode. In WCMP load balancing mode, the default value of *weight* is **1** if *weight* is not specified for the **next-hop** address.

Examples

The following example configures the route map **load-balance** to forward packets received by GigabitEthernet 0/1 from the network segment 10.0.0.0/8, to 192.168.100.1, forward packets received from the network segment 172.16.0.0/16 to 172.16.100.1, and drop other packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip policy route-map load-balance
Hostname(config)# access-list 10 permit 10.0.0.0 0.255.255.255
Hostname(config)# access-list 20 permit 172.16.0.0 0.0.255.255
Hostname(config)#route-map load-balance permit 10
Hostname(config-route-map)# match ip address 10
Hostname(config-route-map)# set ip next-hop 192.168.100.1
Hostname(config)#route-map load-balance permit 20
Hostname(config-route-map)# match ip address 20
Hostname(config-route-map)# set ip next-hop 172.16.100.1
Hostname(config)#route-map load-balance permit 30
Hostname(config-route-map)# set interface Null 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 set ip next-hop recursive

Function

Run the **set ip next-hop recursive** command to specify the recursive next-hop IP address for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no recursive next-hop IPv4 address is specified for matched packets.

Syntax

set ip next-hop recursive *ipv4-address*

no set ip next-hop recursive

Parameter Description

ipv4-address: Recursive next-hop IP address.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration. You can configure only one such **set** command in a route map policy.

The recursive next-hop IP addresses can be recursively sought in static or dynamic routes that have an outbound interface and a next-hop IP address. Recursion can be performed up to 32 times. If the recursive next-hop IP address is sought in a static route, recursion can be performed only once.

Examples

The following example configures the route map **load-balance** to forward packets received by GigabitEthernet 0/1 from the network segment 10.0.0.0/8 to the recursive next hop 192.168.100.1, forward packets received from the network segment 172.16.0.0/16 to the recursive next hop 172.16.100.1, and forward other packets based on the common routes by default.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip policy route-map load-balance
Hostname(config)#access-list 10 permit 10.0.0.0 0.255.255.255
Hostname(config)#access-list 20 permit 172.16.0.0 0.0.255.255
Hostname(config)#route-map load-balance permit 10
Hostname(config-route-map)#match ip address 10
Hostname(config-route-map)#set ip next-hop recursive 192.168.100.1
Hostname(config)#route-map load-balance permit 20
Hostname(config-route-map)#match ip address 20
Hostname(config-route-map)#set ip next-hop recursive 172.16.100.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pbr route** (PBR)

1.43 set ip next-hop self

Function

Run the **set ip next-hop self** command to set the next hop to the device itself for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the next hop is not set to the device itself for matched packets.

Syntax

set ip next-hop self

no set ip next-hop self

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to the device itself.

Examples

The following example configures the route map **abc** to set the next hop to the device itself, and applies this route map to routes advertised to the neighbor 1.1.1.1 in AS 65000 in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set ip next-hop self
Hostname(config)#router bgp 65000
Hostname(config-router)#neighbor 1.1.1.1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.44 set ip next-hop unchanged

Function

Run the **set ip next-hop unchanged** command to set the next hops of routes that match the rules to keep unchanged.

Run the **no** form of this command to remove this configuration.

By default, the next hop is not set to keep unchanged for a matched packet. This command is used for route map management in BGP.

Syntax

set ip next-hop unchanged

no set ip next-hop unchanged

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to keep unchanged.

Examples

The following example configures the route map **abc** to set the next hop to keep unchanged, and applies this route map to the routes sent to the neighbor 1.1.1.1 in AS 65000 in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set ip next-hop unchanged
Hostname(config)#router bgp 65000
Hostname(config-router)#neighbor 1.1.1.1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 set ip next-hop verify-availability

Function

Run the **set ip next-hop verify-availability** command to verify availability of the next-hop IPv4 address.

Run the **no** form of this command to remove this configuration.

By default, availability of the next-hop IPv4 address is not verified for matched packets.

Syntax

set ip next-hop verify-availability *ipv4-address* [*weight*] { **track** *track-obj-number* | **bfd** *interface-type interface-number gateway* }

no set ip next-hop verify-availability *ipv4-address* [*weight*] { **track** *track-obj-number* | **bfd** *interface-type interface-number gateway* }

Parameter Description

ipv4-address: IP address of the next hop.

weight: Weight in the load balancing mode. The value range is from 1 to 8.

track: Checks whether the next hop is effective by means of tracking.

track-obj-number: Number of the tracked object. The value range is from 1 to 700.

bfd: Specifies that Bidirectional Forwarding Detection (BFD) is used for neighbor detection.

interface-type: Interface type.

interface-number: Interface number.

gateway: IP address of the gateway, which is the neighbor IP address of BFD. If the next hop is set to the neighbor, BFD is used to detect availability of the forwarding path.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration to verify availability of the next-hop IPv4 address.

Examples

The following example configures the route map **rmap** to verify availability of the next hop 192.168.1.2 by using a tracked object with the number of 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map rmap permit 10
Hostname(config-route-map)# set ip next-hop verify-availability 192.168.1.2 track 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 set ip precedence

Function

Run the **set ip precedence** command to configure the priority of the IPv4 header for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no IPv4 header priority is configured for matched packets.

Syntax

set ip precedence { *precedence* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

no set ip precedence

Parameter Description

precedence: Priority of an IPv4 header indicated by a number. The value range is from 0 to 7.

7: critical

6: flash

5: flash-override

4: immediate

3: internet

2: network

1: priority

0: routine

critical | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**: Specifies the priority of an IP header.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

The priority of the IP packet header is configured so that IP packets are routed based on different priorities during PBR.

You can configure multiple **set ip precedence** commands in a route map policy, but only the last command takes effect, and a priority is specified for the header of a matched IP packet during PBR.

Examples

The following example configures the route map **name** to set the precedence of packets matching ACL 1 (source address: 192.168.217.68) to 4, and applies the route map to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.217.68 0.0.0.0
Hostname(config)# route-map name
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set ip precedence 4
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip policy route-map name
```

Notifications

If you configure this command after the **set ip dscp** command has been configured, the following notification will be displayed:

```
% Route-map: can not set ip precedence.
% Remove set ip dscp clause before set ip precedence.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 set ip tos

Function

Run the **set ip tos** command to configure the ToS of the IPv4 header for a packet that matches the rules.

Run the **no** form of this command to remove this configuration.

By default, no ToS is configured for the IP header of a matched packet.

Syntax

set ip tos { *tos-number* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }

no set ip tos

Parameter Description

tos-number: ToS of an IPv4 header indicated by a number. The value range is from 0 to 15.

max-reliability | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**: ToS of an IPv4 header. The ToS values correspond to numbers as follows:

max-reliability: 2

max-throughput: 4

min-delay: 8

min-monetary-cost: 1

normal: 0

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

The ToS of the IP packet header is configured to deliver different quality of service (QoS) for IP packets that are routed using PBR. A ToS value is specified for the header of a matched IP packet during PBR.

Examples

The following example configures the route map **name** to set the ToS of packets matching ACL 1 (source address: 192.168.217.68) to 4, and applies the route map to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.217.68 0.0.0.0
Hostname(config)# route-map name
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set ip tos 4
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip policy route-map name
```

Notifications

If you configure this command after the **set ip dscp** command has been configured, the following notification will be displayed:

```
% Route-map: can not set ip tos.
% Remove set ip dscp clause before set ip tos.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.48 set ipv6 default next-hop

Function

Run the **set ipv6 default next-hop** command to specify the default next-hop IPv6 address for IPv6 packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no default next-hop IPv6 address is specified for matched routes.

Syntax

set ipv6 default next-hop { *ipv6-address* [*weight*] }&<1-32>

no set ipv6 default next-hop [*ipv6-address* [*weight*]]&<1-32>

Parameter Description

{ *ipv6-address* [*weight*] }&<1-32>: &<1-32> indicates that you can enter the parameter up to 32 times in this command.

ipv6-address: Next-hop IPv6 address for packet forwarding. The next hop must be an adjacent device.

weight: Weight in load balancing mode. The value range is from 1 to 8.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration. After PBR is applied to an interface, if the routing table does not contain the common route (that is, non-default route) to the destination address of an IPv6 packet that matches the related rules, the packet is forwarded to the next hop specified by the **set ipv6 default nexthop** command; otherwise, the packet is forwarded based on the common route. Note that the rules here are IPv6-related rules.

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system performs WCMP load balancing on traffic based on the configured *weight*.

Restrictions and guidelines:

- You can configure up to 32 IP addresses in this command.
- If the weight of the next hop is specified, you can configure up to four next-hop addresses.
- If **vrf** *vrf-name* is specified, packets are forwarded across VRF instances.
- If **global** is specified, packets are forwarded from the VRF instance to the public network.
- If [**vrf** *vrf-name* | **global**] is not specified, the VRF instance is inherited when the IPv6 packet is forwarded, that is, the next hop belongs to the VRF instance that receives the IPv6 packet.

When an egress of packets is selected based on policy-based routing and the routing table, the priorities are as follows:

set ipv6 next-hop > Common route (non-default route) > **set ipv6 default next-hop** > Default route.

Note

- This function does not take effect on network segments with the mask length exceeding 64.
- When you configure this command together with **set ipv6 next-hop verify-availability**, the next hop configured in **set ipv6 next-hop verify-availability** takes effect first.
- If you configure *weight* after any next-hop address, the operation mode of this **set** command is automatically changed to WCMP. In WCMP load balancing mode, the default value of *weight* is **1** if *weight* is not specified for the **next-hop** address.

Examples

The following example configures the route map **rm_if_0_0** to set the default next hop of traffic that matches IPv6 ACL **acl_for_pbr** (destination address: 2001:0db8:2001:1760::/64) to **2002:0db8:2003:1::95**, and applies the route map to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl_for_pbr
Hostname(config -ipv6-acl)# permit ipv6 any 2001:0db8:2001:1760::/64
Hostname(config)# route-map rm_if_0_0
Hostname(config-route-map)# match ipv6 address acl_for_pbr
Hostname(config-route-map)# set ipv6 default next-hop
2002:0db8:2003:1::95
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 policy route-map rm_if_0_0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 set ipv6 next-hop

Function

Run the **set ipv6 next-hop** command to specify the next-hop IPv6 address for IPv6 packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no next-hop IPv6 address is specified for a matched route.

Syntax

set ipv6 next-hop { *ipv6-address* [*weight*] }&<1-32>

no set ipv6 next-hop [*ipv6-address* [*weight*]]&<1-32>

Parameter Description

{ *ipv6-address* [*weight*] }&<1-32>: &<1-32> indicates that you can enter the parameter up to 32 times in this command.

ipv6-address: Next-hop IPv6 address for packet forwarding. The next hop must be an adjacent device.

weight: Weight in load balancing mode. The value range is from 1 to 8.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration. This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system performs WCMP load balancing on traffic based on the configured *weight*.

Restrictions and guidelines:

- You can configure up to 32 IP addresses in this command.
- If the weight of the next hop is specified, you can configure up to four next-hop addresses.
- If **vrf** *vrf-name* is specified, packets are forwarded across VRF instances.
- If **global** is specified, packets are forwarded from the VRF instance to the public network.
- If [**vrf** *vrf-name* | **global**] is not specified, the VRF instance is inherited when the IPv6 packet is forwarded, that is, the next hop belongs to the VRF instance that receives the IPv6 packet.

Note

If you configure *weight* after any next-hop address, the operation mode of this **set** command is automatically changed to WCMP. In WCMP load balancing mode, the default value of *weight* is **1** if *weight* is not specified for the **next-hop** address.

When an egress of packets is selected based on policy-based routing and the routing table, the priorities are as follows:

set ipv6 next-hop > **set ipv6 next-hop recursive >** Common route (non-default route) > **set ipv6 default next-hop** > Default route

Examples

The following example configures the route map **rm_if_0_0** to set the next-hop address of traffic that matches IPv6 ACL **acl_for_pbr** (destination address: 2001:0db8:2001:1760::/64) to **2002:0db8:2003:1::95**, and applies the route map to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl_for_pbr
Hostname(config -ipv6-acl)# permit ipv6 any 2001:0db8:2001:1760::/64
Hostname(config)# route-map rm_if_0_0
Hostname(config-route-map)# match ip address acl_for_pbr
Hostname(config-route-map)# set ipv6 next-hop 2002:0db8:2003:1::95
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 policy route-map rm_if_0_0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 set ipv6 next-hop recursive

Function

Run the **set ipv6 next-hop recursive** command to specify the recursive next-hop IPv6 address for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no recursive next-hop IPv6 address is specified for matched packets.

Syntax

set ipv6 next-hop recursive *ipv6-address*

no set ipv6 next-hop recursive

Parameter Description

ipv6-address: Recursive next-hop IPv6 address.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration. You can configure only one such **set** command in a route map policy.

The recursive next-hop IPv6 addresses can be recursively sought in static or dynamic routes that have an outbound interface and a next-hop IPv6 address. Recursion can be performed up to 32 times. If the recursive next-hop IPv6 address is sought in a static route, recursion can be performed only once.

Examples

The following example configures the route map **rm_if_0_0** to set the recursive next-hop address of traffic that matches IPv6 ACL **acl_for_pbr** (destination address: 2001:0db8:2001:1760::/64) to **2002:0db8:2003:1::95**, and applies the route map to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl_for_pbr
Hostname(config -ipv6-acl)# permit ipv6 any 2001:0db8:2001:1760::/64
Hostname(config)# route-map rm_if_0_0
Hostname(config-route-map)# match ip address acl_for_pbr
Hostname(config-route-map)# set ipv6 next-hop recursive 2002:0db8:2003:1::95
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 policy route-map rm_if_0_0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pbr route** (PBR)

1.51 set ipv6 next-hop self

Function

Run the **set ipv6 next-hop self** command to set the next hop to the device itself for IPv6 routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the next hop is not set to the device itself for matched packets.

Syntax

set ipv6 next-hop self

no set ipv6 next-hop self

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to the device itself.

Examples

The following example configures the route map **abc** to set the next hop of routes to the device itself, and applies the rout map to routes advertised to the neighbor 2001::1 in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set ipv6 next-hop self
Hostname(config)#router bgp 65000
Hostname(config-router)#neighbor 2001::1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 set ipv6 next-hop unchanged

Function

Run the **set ipv6 next-hop unchanged** command to set the next hop to keep unchanged for IPv6 routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the next hop is not set to keep unchanged for a matched packet. This command is used for route map management in BGP.

Syntax

set ipv6 next-hop unchanged

no set ipv6 next-hop unchanged

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to keep unchanged.

Examples

The following example configures the route map **abc** to set the next hops of routes to keep unchanged, and applies the rout map to routes advertised to the neighbor 2001::1 in BGP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set ipv6 next-hop unchanged
Hostname(config)#router bgp 1
Hostname(config-router)#neighbor 2001::1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 set ipv6 next-hop verify-availability

Function

Run the **set ipv6 next-hop verify-availability** command to verify availability of the next-hop IPv6 address.

Run the **no** form of this command to remove this configuration.

By default, availability of the next-hop IPv6 address is not verified for matched packets.

Syntax

set ipv6 next-hop verify-availability *ipv6-address* [*weight*] **bfd** *interface-type interface-number gateway*

no set ip next-hop verify-availability *ipv6-address* [*weight*] **bfd** *interface-type interface-number gateway*

Parameter Description

ipv6-address: IPv6 address of the next hop.

weight: Weight in load balancing mode. The value range is from 1 to 8.

bfd: Specifies that BFD is used for neighbor detection.

interface-type: Interface type.

interface-number: Interface number.

gateway: IPv6 address of the gateway, that is, the IPv6 address of the BFD neighbor. If the next hop is set to the neighbor, BFD is used to detect availability of the forwarding path.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration to verify availability of the next-hop IPv6 address.

Examples

The following example configures a route map to associate with BFD, and uses BFD to verify availability of 2001:1::2, which is the next hop of the forwarding path.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map rmap permit 10
Hostname(config-route-map)# set ipv6 next-hop verify-availability 2001:1::2 bfd
GigabitEthernet 0/1 2001:1::2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 set ipv6 precedence

Function

Run the **set ipv6 precedence** command to configure the priority of the IPv6 header for packets that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no IPv6 header priority is configured for matched packets.

Syntax

set ipv6 precedence { *precedence-number* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

no set ipv6 precedence

Parameter Description

precedence-number: Priority of an IP header indicated by a number. The value range is from 0 to 7.

7: critical

6: flash

5: flash-override

4: immediate

3: internet

2: network

1: priority

0: routine

critical | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**: Specifies the priority of an IP header.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

The priority of the IPv6 packet header is often configured so that IP packets are routed based on different priorities during PBR.

You can configure multiple **set ipv6 precedence** commands in a route map policy, but only the last command takes effect, and a priority is specified for the header of a matched IP packet during PBR.

Examples

The following example configures a route map to change the priority of IPv6 packet headers to **3**.

```
Hostname(config)#route-map pbr-aaa permit 10
Hostname(config-route-map)# set ipv6 precedence 3
```

The following example configures a route map to change the priority of IPv6 packet headers to **immediate**.

```
Hostname(config-route-map)# set ipv6 precedence immediate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 set l3vpn nexthop local-vrf

Function

Run the **set l3vpn nexthop local-vrf** command to set the L3 VPN next hop to the local VRF instance for packets matching the match rules.

Run the **no** form of this command to remove this configuration.

By default, the L3 VPN next hop is not set to the local VRF instance for packets matching the rules.

Syntax

set l3vpn nexthop local-vrf

no set l3vpn nexthop local-vrf

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the route map **test** to set the L3 VPN next hop to the local VRF instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map test
Hostname(config-route-map)# set l3vpn nexthop local-vrf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 set level

Function

Run the **set level** command to specify the type of the destination area to which routes that match the rules will be advertised.

Run the **no** form of this command to remove this configuration.

By default, the type of the destination area is not specified for matched routes.

Syntax

set level { **level-1** | **level-1-2** | **level-2** | **stub-area** | **backbone** }

no set level

Parameter Description

level-1: Advertises redistributed routes to an IS-IS level-1 area.

level-2: Advertises redistributed routes to an IS-IS level-2 area.

level-1-2: Advertises redistributed routes to IS-IS level-1 and level-2 areas.

stub-area: Advertises redistributed routes to an OSPF stub area.

backbone: Advertises redistributed routes to the OSPF backbone area.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

When routes are redistributed to the OSPF network or IS-IS hierarchical network, this command is used to configure the type of the area to which the redistributed routes are to be advertised.

Examples

The following example configures the route map **redrip** to set the type of the destination area, to which the redistributed routes are to be advertised, to the backbone area, and redistribute RIP routes to the OSPF backbone area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# set level backbone
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 set local-preference

Function

Run the **set local-preference** command to configure the LOCAL_PREFERENCE value for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no LOCAL_PREFERENCE value is configured for matched routes.

Syntax

set local-preference *precedence-number*

no set local-preference

Parameter Description

precedence-number: LOCAL_PREFERENCE value indicated by a number. The value range is from 0 to 4294967295.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the local priority for matched routes. You can configure only one LOCAL_PREFERENCE value.

Examples

The following example configures a route map to set LOCAL_PREFERENCE of routes that match ACL 1 to a high priority **6800** in the policy with the sequence number of 10, and set LOCAL_PREFERENCE of routes that match ACL 2 to a low priority **50** in the policy with the sequence number of 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map SET_PREF permit 10
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set local-preference 6800
Hostname(config-route-map)# exit
```

```
Hostname(config)# route-map SET_PREF permit 20
Hostname(config-route-map)# match as-path 2
Hostname(config-route-map)# set local-preference 50
```

Related Commands

N/A

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.58 set metric

Function

Run the **set metric** command to configure the metric value for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the metric of a matched route is not modified.

Syntax

set metric { **+** *metric-value* | **-** *metric-value* | *metric-value* }

no set metric

Parameter Description

+: Increases the metric (on the basis of the metric value of the original route).

-: Decreases the metric (on the basis of the metric value of the original route).

metric-value: Metric value of a redistributed route. The value range is from 0 to 4294967295.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

The route metric affects route selection. Therefore, configure it carefully based on the actual network topology. Pay attention to the upper and lower limits of the metric in each routing protocol when configuring, increasing, or decreasing the metric. For example, when routes of other protocols are redistributed to RIP, the metric falls within the range of 1 to 16 after metric increase/decrease.

Examples

The following example configures the route map **redrip** to set the initial route metric to 40 and change the metric based on the route map **redrip** when RIP routes are redistributed to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# set metric 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 set metric-type

Function

Run the **set metric-type** command to configure the metric type for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the metric type of a matched route is not modified.

Syntax

set metric-type { **external** | **internal** | **type-1** | **type-2** }

no set metric-type

Parameter Description

external: Specifies the external route type of OSPF.

internal: Specifies the internal route type of OSPF.

type-1: Specifies external OE1 route type of OSPF.

type-2: Specifies the external OE2 route type of OSPF.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to modify the OSPF route type. You can use it for route redistribution or PBR.

Examples

The following example configures the route map **redrip** to set the route type to **type-1**, and change the route type based on the route map **redrip** when RIP routes are redistributed to OSPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# set metric-type type-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 set next-hop

Function

Run the **set next-hop** command to specify the next-hop IP address for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no next-hop IP address is specified for matched routes.

Syntax

set next-hop *ipv4-address*

no set next-hop

Parameter Description

ipv4-address: IPv4 address of the next hop.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used only for PBR configuration. You can use it to flexibly adjust the next hop of a route based on the matching conditions.

Examples

The following example configures the route map **redrip** to set the next hop of routes that match ACL 1 to 192.168.1.2

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set next-hop 192.168.1.2
```

Notifications

If the configured IP address is an invalid host address (valid host addresses include class A addresses except those starting with 0 or 127, class B addresses, and class C addresses), the following notification will be displayed:

```
% Can't set invalid nexthop address!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 set next-hop self

Function

Run the **set next-hop self** command to set the next hop to the device itself for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, the next hop is not set to the device itself for matched routes.

Syntax

set next-hop self

no set next-hop self

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to the device itself.

Examples

The following example configures the route map **abc** to set the next hop of a BGP route to the device itself, and applies the route map **abc** when BGP 65000 advertises routes to the neighbor 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set next-hop self
Hostname(config)#router bgp 65000
Hostname(config-router)#neighbor 1.1.1.1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 set next-hop unchanged

Function

Run the **set next-hop unchanged** command to set the next hop to keep unchanged for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no next hop is set to keep unchanged for matched routes. This command is used for route map management in BGP.

Syntax

set next-hop unchanged

no set next-hop unchanged

Parameter Description

N/A

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a route map to associate with BGP, and set the next hops of routes to be sent to keep unchanged.

Examples

The following example configures the route map abc to set the next hop of a BGP route to keep unchanged, and applies the route map when BGP 1 advertises routes to the neighbor 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#route-map abc
Hostname(config-route-map)#set next-hop unchanged
Hostname(config)#router bgp 1
Hostname(config-router)#neighbor 1.1.1.1 route-map abc out
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 set origin

Function

Run the **set origin** command to specify the source for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no route source is specified for matched routes.

Syntax

set origin { **egp** | **igp** | **incomplete** }

no set origin

Parameter Description

egp: Specifies that the source is the remote EGP.

igp: Specifies that the source is the local IGP.

incomplete: Specifies that the route source is unknown.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the source for a matched route. You can configure only one route source.

Examples

The following example configures the route map **SET_ORIGIN** to set the route source to **igp** for routes that match ACL 1 in the policy with the sequence number of 10, and set the route source to **egp** for routes that match ACL 2 in the policy with the sequence number of 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map SET_ORIGIN 10 permit
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set origin igp
Hostname(config-route-map)# exit
Hostname(config)# route-map SET_ORIGIN 20 permit
Hostname(config-route-map)# match as-path 2
Hostname(config-route-map)# set origin egp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 set originator-id

Function

Run the **set originator-id** command to specify the originator address for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no route originator address is configured for matched routes.

Syntax

set originator-id *ipv4-address*

no set originator-id [*ipv4-address*]

Parameter Description

ipv4-address: Address of the originator.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the originator address for a matched route.

Examples

The following example configures the route map **SET_ORIGIN** to set the originator address to **5.5.5.5** for routes that match ACL 1 in the policy with the sequence number of 10 and set the originator address to **5.5.5.6** for routes that match ACL 2 in the policy with the sequence number of 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map SET_ORIGIN 10 permit
Hostname(config-route-map)# match as-path 1
Hostname(config-route-map)# set originator-id 5.5.5.5
Hostname(config-route-map)# exit
Hostname(config)# route-map SET_ORIGIN 20 permit
Hostname(config-route-map)# match as-path 2
Hostname(config-route-map)# set originator-id 5.5.5.6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.65 set qos-id

Function

Run the **set qos-id** command to specify the QoS ID for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no QoS ID is specified for matched routes.

Syntax

set qos-id *qos-id*

no set qos-id

Parameter Description

qos-id: QoS ID of a route. The value range is from 1 to 255.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used for PBR configuration in BGP to set the QoS ID for routes.

This command supports only one parameter (QoS ID), and does not support the configuration of multiple QoS IDs.

Examples

The following example sets the QoS ID of routes that match the rules to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# route-map test
Hostname(config-route-map)# set qos-id 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 set tag

Function

Run the **set tag** command to configure the tag for routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no route tag is configured for matched routes.

Syntax

set tag *tag*

no set tag

Parameter Description

tag: Tag of a redistributed route. The value range is from 0 to 4294967295.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is applicable only to route redistribution. If this command is not configured, the original route tag is retained.

Examples

The following example configures the route map **redip** to set the tag to **100** for routes that match the rules, configure OSPF to redistribute RIP routes based on the route map **redip**, and set the tag of redistributed routes to **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf
Hostname(config-router)# redistribute rip subnets route-map redrip
Hostname(config-router)# network 192.168.12.0 0.0.0.255 area 0
Hostname(config-router)# exit
Hostname(config)# route-map redrip permit 10
Hostname(config-route-map)# set tag 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.67 set weight

Function

Run the **set weight** command to configure the weight for BGP routes that match the rules.

Run the **no** form of this command to remove this configuration.

By default, no weight is configured for matched routes.

Syntax

set weight *weight-number*

no set weight

Parameter Description

weight-number: Weight of a route. The value range is from 0 to 65535.

Command Modes

Route map configuration mode

Default Level

14

Usage Guidelines

This command is only used to modify the weight of a BGP route.

By default, the weight of a route received from a neighbor is obtained based on the configuration of **neighbor weight**, and the weight of a local route is always 32768.

You can run this command to modify the default weight allocated by BGP.

Examples

The following example configures the route map **nei-rmap-in** to set the weight to **100** for BGP routes that match the rules, and applies this route map when routes sent from the BGP neighbor 1.1.1.1 are received.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router bgp 1
Hostname(config-router)# neighbor 1.1.1.1 route-map nei-rmap-in in
Hostname(config-router)# exit
Hostname(config)# route-map nei-rmap-in permit 10
Hostname(config-route-map)# set weight 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 show ip as-path-access-list

Function

Run the **show ip as-path-access-list** command to display the AS-path list information.

Syntax

show ip as-path-access-list [*as-path-access-list-num*]

Parameter Description

as-path-access-list-num: Number of an AS-path list. The value range is from 1 to 500.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the AS-path list information.

Examples

The following example displays the information about all AS path lists.

```
Hostname> enable
Hostname# show ip as-path-access-list
AS path access list 30
permit ^30$
```

Table 1-1 Output Fields of the show ip as-path-access-list Command

Field	Description
AS path access list	Name of an AS-path list
permit	Mode of a filtering rule
^30$	Specific rule indicated by a regular expression

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.69 show ip community-list

Function

Run the **show ip community-list** command to display the community list information.

Syntax

show ip community-list [*community-list-number* | *community-list-name*]

Parameter Description

community-list-number: Number of a community list to be displayed. For a standard community list, the range is from 1 to 99. For an expanded community list, the range is from 100 to 199.

community-list-name: Name of a community list to be displayed.

It is a string of less than 80 characters.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the community list information.

Examples

The following example displays the information about all community lists.

```
Hostname> enable
Hostname# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Table 1-2 Output Fields of the show ip community-list Command

Field	Description
Community-list standard local	Type and name of a community list
permit	Mode of a filtering rule
local-AS	Value of the community attribute
0:10	Value of the community attribute

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.70 show ip extcommunity-list

Function

Run the **show ip extcommunity-list** command to display the extcommunity list information.

Syntax

show ip extcommunity-list [*extcommunity-list-num* | *extcommunity-list-name*]

Parameter Description

extcommunity-list-num: Number of an extcommunity list, which identifies a standard or expanded extcommunity list. The value range is from 1 to 199. For a standard extcommunity list, the range is from 1 to 99. For an expanded extcommunity list, the range is from 100 to 199.

extcommunity-list-num: Name of a standard or expanded extcommunity list.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information about all extcommunity lists.

```
Hostname> enable
```

```
Hostname # show ip extcommunity-list
Standard extended community-list 1
    10 permit RT:1:200
    20 permit RT:1:100
Standard extended community-list 2
    10 permit RT:1:200
Expanded extended community-list rt_filter
    13 permit 1:100
```

Table 1-3 Output Fields of the show ip extcommunity-list Command

Field	Description
Standard extended community-list 1	Type and name of an extcommunity list
10	Sequence number of a filtering rule
permit	Mode of a filtering rule
RT:1:200	Value of the extcommunity attribute

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.71 show ip prefix-list

Function

Run the **show ip prefix-list** command to display the information about a prefix list or prefix list entries.

Syntax

show ip prefix-list [*prefix-name*]

Parameter Description

prefix-name: Name of a prefix list.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no prefix list name is specified, the configurations of all prefix lists are displayed. Otherwise, only configurations of the specified prefix list are displayed.

Examples

The following example displays the information of all IPv4 prefix lists.

```
Hostname> enable
Hostname# show ip prefix-list
ip prefix-list pre: 2 entries
seq 5 permit 192.168.64.0/24
seq 10 permit 192.2.2.0/24
```

Table 1-4 Output Fields of the show ip prefix-list Command

Field	Description
ip prefix-list pre	Name of an IPv4 prefix list
2 entries	Number of rules in the prefix list
seq 5	Sequence number of a filtering rule
permit	Mode of a filtering rule
192.168.64.0/24	IPv4 route prefix

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.72 show ip protocols

Function

Run the **show ip protocols** command to display the status information of the IPv4 routing protocols that are currently running.

Syntax

show ip protocols [**vrf** *vrf-name*] [**bgp** | **isis** | **ospf** | **rip**]

Parameter Description

vrf *vrf-name*: Specifies the name of a VRF instance. If this parameter is not specified, the status information of running routing protocols in the global VRF instance is displayed.

bgp: Displays status information of the BGP protocol.

isis: Displays status information of the ISIS protocol.

ospf: Displays status information of the OSPF protocol.

rip: Displays status information of the RIP protocol.

If no keyword is configured after **protocols**, the status information of all running routing protocols is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Only the status information of running routing protocols is displayed, and that of disabled routing protocols is not displayed.

Examples

The following example displays the status information of running routing protocols in the global VRF instance.

```
Hostname> enable
Hostname# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 57.57.57.57
  Memory Overflow is enabled
  Router is not in overflow state now
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    bgp, includes subnets in redistribution
  Number of areas in this router is 2: 2 normal 0 stub 0 nssa
  Routing for Networks:
    57.57.57.57 0.0.0.0 area 0
    163.18.4.0 0.0.0.255 area 0
    163.18.57.0 0.0.0.255 area 0
    192.100.1.0 0.0.0.255 area 0
    192.101.1.0 0.0.0.255 area 1
    192.102.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)
Routing Protocol is "bgp 10"
  IGP synchronization is disabled
  Default-information originate is disabled
  Default local-preference applied to incoming route is 100
  Redistributing: connected
```

```
 Neighbor(s):
   Address          AddressFamily  FiltIn  FiltOut  DistIn  DistOut  RouteMapIn
RouteMapOut  Weight
 Distance: external 20(default) internal 200(default) local 200(default)
```

Table 1-5 Output Fields of the show ip protocols Command

Field	Description
Routing Protocol is "ospf 1"	Name of a routing protocol
Redistributing External Routes from	Route redistribution status of the routing protocol
Distance:	Distance of the routing protocol
Router ID	Unique ID of the device
Memory Overflow	Whether the memory overflow alarm function is enabled
Number of areas in this router	Number of areas where the routing protocol is applied
Routing for Networks	Area distribution of interfaces where the current routing protocol is applied
Reference bandwidth unit	Reference bandwidth unit of the interface cost
IGP synchronization	IGP synchronization function
Default-information originate	Allows the BGP speaker to advertise the default route to the peer group.
Default local-preference applied to incoming route	Default local-preference value
Redistributing	Route redistribution type
Neighbor(s)	BGP neighbor list
Address	Address of a BGP neighbor
AddressFamily	Address family of a BGP neighbor
FiltIn	AS filtering in the inbound direction
FiltOut	AS filtering in the outbound direction
DistIn	ACL filtering in the inbound direction
DistOut	ACL filtering in the outbound direction
RouteMapIn	Routing policy in the inbound direction
RouteMapOut	Routing policy in the outbound direction
Weight	Weight used by a neighbor

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.73 show ipv6 prefix-list

Function

Run the **show ipv6 prefix-list** command to display the information about an IPv6 prefix list or prefix list entries.

Syntax

show ipv6 prefix-list [*prefix-name*]

Parameter Description

prefix-name: Name of an IPv6 prefix list.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no prefix list name is specified, the configurations of all prefix lists are displayed. Otherwise, only configurations of the specified prefix list are displayed.

Examples

The following example displays the information about all IPv6 prefix lists.

```
Hostname> enable
Hostname# show ipv6 prefix-list
ipv6 prefix-list p6: 2 entries
     seq 5 permit 13::/20
     seq 10 permit 14::/20
```

Table 1-6 Output Fields of the show ipv6 prefix-list Command

Field	Description
ipv6 prefix-list p6	Name of an IPv6 prefix list
2 entries	Number of rules in the prefix list
seq 5	Sequence number of a filtering rule

Field	Description
permit	Mode of a filtering rule
13::/20	IPv6 route prefix

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.74 show route-map

Function

Run the **show route-map** command to display the route map configurations.

Syntax

show route-map [*route-map-name*]

Parameter Description

route-map-name: Name of a route map to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no route map name is specified, the configurations of all route maps are displayed. Otherwise, only configurations of the specified route map are displayed.

Examples

The following example displays the route map information.

```
Hostname> enable
Hostname# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Table 1-7 Output Fields of the show route-map Command

Field	Description
route-map	Name of a route map
permit	Permit keyword contained in a route map policy
sequence 10	Sequence number of a route map policy
match clauses	Match rule. Whether the **set** operation is performed depends on the **permit** or **deny** keyword in the route map policy.
set clauses	Processing action to be performed after the match rule is matched.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 PBR Commands

Command	Function
clear ip pbr statistics	Clear the statistics about packets forwarded by the IPv4 Policy-Based Routing (PBR).
clear ipv6 pbr statistics	Clear the statistics about packets forwarded by the IPv6 PBR.
ip local policy route-map	Apply PBR to packets sent by the local device.
ip policy	Configure redundant backup or load balancing among multiple next hops for PBR.
ip policy route-map	Apply PBR to an interface.
ip policy-source in-interface	Apply source-address-based PBR to IPv4 packets received by a specified interface.
ipv6 local policy route-map	Apply PBR to IPv6 packets sent by the local device.
ipv6 policy	Configure redundant backup or load balancing among multiple next hops for PBR.
ipv6 policy route-map	Apply the IPv6 PBR to an interface.
ipv6 policy-source in-interface	Apply source-address-based PBR to IPv6 packets received by a specified interface.
show ip pbr bfd	Display the correlation between the IPv4 PBR and BFD.
show ip pbr route	Display the IPv4 PBR applied to an interface.
show ip pbr route-map	Display the route map information of IPv4 PBR.
show ip pbr source-route	Display the routing information of the source-address-based IPv4 PBR.
show ip pbr statistics	Display the statistics about packets forwarded by the IPv4 PBR.
show ip policy	Display interfaces for which the PBR is configured and the name of the route map applied to each interface.
show ipv6 pbr bfd	Display the correlation between the IPv6 PBR and BFD.

show ipv6 pbr route	Display the IPv6 PBR applied to an interface.
show ipv6 pbr route-map	Display the route map information of IPv6 PBR.
show ipv6 pbr source-route	Display the routing information of the source-address-based IPv6 PBR.
show ipv6 pbr statistics	Display the statistics about packets forwarded by the IPv6 PBR.
show ipv6 policy	Display interfaces for which the IPv6 PBR is configured and the name of the route map applied to each interface.

1.1 clear ip pbr statistics

Function

Run the **clear ip pbr statistics** command to clear the statistics about packets forwarded by the IPv4 Policy-Based Routing (PBR).

Syntax

clear ip pbr statistics [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Clears the statistics about packets forwarded by the IPv4 PBR on the specified interface. If optional parameters are not specified, the statistics about packets forwarded by all interfaces to which the IPv4 PBR applies is cleared.

local: Clears the statistics about packets forwarded by the IPv4 PBR on a local interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can run this command to clear the statistics about packets forwarded by the IPv4 PBR.

Examples

The following example clears the statistics about packets forwarded by the IPv4 PBR.

```
Hostname# enable
Hostname# clear ip pbr statistics
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 pbr statistics

Function

Run the **clear ipv6 pbr statistics** command to clear the statistics about packets forwarded by the IPv6 PBR.

Syntax

clear ipv6 pbr statistics [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Clears the statistics about packets forwarded by the IPv6 PBR on the specified interface. If optional parameters are not specified, the statistics about packets forwarded by all interfaces to which the IPv6 PBR applies is cleared.

local: Clears the statistics about packets forwarded by the IPv6 PBR on a local interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can run this command to clear the statistics about packets forwarded by the IPv6 PBR.

Examples

The following example clears the statistics about packets forwarded by the IPv6 PBR.

```
Hostname> enable
Hostname# clear ipv6 pbr statistics
```

Notifications

N/A

Platform Description

N/A

1.3 ip local policy route-map

Function

Run the **ip local policy route-map** command to apply PBR to packets sent by the local device.

Run the **no** form of this command to remove this configuration.

By default, no PBR is applied to the local device.

Syntax

ip local policy route-map *route-map-name*

no ip local policy route-map

Parameter Description

route-map-name: Name of the route map.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command enables PBR for only IP packets that are sent by the local device and match the policy. It is not applicable to IP packets received by the local device.

To apply PBR, you must specify a route map for PBR, and create this map. A route map consists of multiple policies, and one or more match rules and relevant actions are defined for each policy. After PBR is applied to an interface, all packets received by the interface are checked. Packets that do not match any policy in the route map are routed and forwarded as usual. Packets that match a policy in the route map are processed based on the action defined in the policy.

Examples

The following example routes all packets from the source address 192.168.217.10 through the GigabitEthernet 0/1 interface.

(1) Step 1: Configure ACL 1 to match packets with the source IP address 192.168.217.10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit host 192.168.217.10
```

(2) Step 2: Configure the route map **lab1**, and send packets that matches ACL 1 from the GigabitEthernet 0/1 interface.

```
Hostname(config)# route-map lab1 permit 10
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set interface GigabitEthernet 0/1
Hostname(config-route-map)# exit
```

(3) Step 3: Apply PBR to packets sent by the local device.

```
Hostname(config)# ip local policy route-map lab1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip policy

Function

Run the **ip policy** command to configure redundant backup or load balancing among multiple next hops for PBR.

Run the **no** form of this command to restore the forwarding mode of PBR.

By default, multiple next hops of the PBR adopt the redundant backup mode.

Syntax

ip policy { load-balance | redundance }

no ip policy

Parameter Description

load-balance: Adopts load balancing.

redundance: Adopts redundant backup.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **set ip next-hop** command to configure multiple next hops. The next-hop selection policy configured by this command is redundant backup or load balancing. When redundant backup is configured, only the first parsed next hop of PBR takes effect. When load balancing is configured, multiple parsed next hops of PBR take effect. You can configure up to 8 next hops in the case of Weighted Cost Multiple Path (WCMP), or 32 next hops in the case of Equal Cost Multiple Path (ECMP).

Caution

The next hop refers to the next hop of which the MAC address is learned.

Examples

The following example configures multiple next hops in the route map and sets the redundant backup mode in global configuration mode so that only the first next hop takes effect after PBR is applied to GigabitEthernet 0/1.

(1) Step 1: Configure ACL 1 to match the traffic from the IP address 10.0.0.1, and ACL 2 to match the traffic from the IP address 20.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit host 10.0.0.1
Hostname(config)# access-list 2 permit host 20.0.0.1
```

(2) Step 2: Configure the sequence number 10 for the route map **lab1**, and set multiple next hops for traffic that matches ACL 1. Configure the sequence number 20 for the route map **lab1**, and set multiple next hops for traffic that matches ACL 2.

```
Hostname(config)# route-map lab1 permit 10
Hostname(config-route-map)# match ip address 1
Hostname(config-route-map)# set ip next-hop 196.168.4.6
Hostname(config-route-map)# set ip next-hop 196.168.4.7
Hostname(config-route-map)# set ip next-hop 196.168.4.8
Hostname(config-route-map)# exit
Hostname(config)# route-map lab1 permit 20
Hostname(config-route-map)# match ip address 2
Hostname(config-route-map)# set ip next-hop 196.168.5.6
Hostname(config-route-map)# set ip next-hop 196.168.5.7
Hostname(config-route-map)# set ip next-hop 196.168.5.8
Hostname(config-route-map)# exit
```

(3) Step 3: Apply PBR to the interface, and configure the redundant backup mode.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if)# ip policy route-map lab1
Hostname(config-if)# exit
Hostname(config)# ip policy redundance
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **set ip next-hop (**routing policy)

1.5 ip policy route-map

Function

Run the **ip policy route-map** command to apply PBR to an interface.

Run the **no** form of this command to remove this configuration.

By default, no PBR is configured on an interface.

Syntax

ip policy route-map *route-map*

no ip policy route-map

Parameter Description

route-map: Name of the route map.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

PBR must be applied to a specified interface and to only packets received by this interface. You can configure only one route map for an interface on a device. If you configure multiple route maps for the same interface, the latest route map overwrites the previous route maps.

To apply PBR, you must specify a route map for PBR, and create this map. A route map consists of multiple policies, and one or more match rules and relevant actions are defined for each policy. After PBR is applied to an interface, all packets received by the interface are checked. Packets that do not match any policy in the route map are routed and forwarded as usual. Packets that match a policy in the route map are processed based on the action defined in the policy.

Examples

The following example configures PBR for packets received by GigabitEthernet 0/0, sets the next hop of packets with the source address 10.0.0.1 to **196.168.4.6** and the next hop of packets with the source address 20.0.0.1 to **196.168.5.6**; otherwise, packets are normally forwarded.

(1) Step 1: Configure ACL 1 to match the traffic from the IP address 10.0.0.1, and ACL 2 to match the traffic from the IP address 20.0.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit host 10.0.0.1
Hostname(config)# access-list 2 permit host 20.0.0.1
```

(2) Step 2: Configure the sequence number 10 for the route map **lab1**, and set the next hop of traffic that matches ACL 1 to **196.168.4.6**. Configure the sequence number 20 for route map **lab1**, and set the next hop of traffic that matches ACL 2 to **196.168.5.6**.

```
Hostname(config)# route-map lab1 permit 10
Hostname (config-route-map)# match ip address 1
Hostname(config-route-map)# set ip next-hop 196.168.4.6
Hostname(config-route-map)# exit
Hostname(config)# route-map lab1 permit 20
Hostname(config-route-map)# match ip address 2
Hostname(config-route-map)# set ip next-hop 196.168.5.6
Hostname(config-route-map)# exit
```

(3) Step 3: Apply PBR to the interface.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if)# ip policy route-map lab1
Hostname(config-if)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip policy-source in-interface

Function

Run the **ip policy-source in-interface** command to apply source-address-based PBR to IPv4 packets received by a specified interface.

Run the **no** form of this command to remove this configuration.

By default, no source-address-based PBR takes effect on an interface.

Syntax

ip policy-source in-interface *interface-type interface-number sequence* { *source-address mask* | *source-address/mask* } { [**default**] **next-hop** [*ipv4-address* [*weight*]]&<1-4> | [**default**] **interface** { *out-interface-type out-interface-number* }&<1-4> }

no ip policy-source in-interface *interface-type sequence* [{ *source-address mask* | *source-address/mask* } [[**default**] **next-hop** [*ipv4-address* [*weight*]]&<1-4> | [**default**] **interface** { *out-interface-type out-interface-number* } &<1-4>]]

Parameter Description

interface-type interface-number: Type and number of the interface to which source-address-based PBR is applied.

sequence: Sequence number of a policy. A smaller sequence number indicates a higher priority.

source-address: IPv4 address.

mask: Mask of the IPv4 address.

default: If this parameter is configured, the system preferentially uses the route forwarding table to forward packets; otherwise, the system preferentially use PBR to forward packets.

next-hop [*ipv4-address* [*weight*]]&<1-4>: You can enter up to four next-hop IPv4 addresses and weight values.

ipv4-address: IPv4 address of the next hop.

weight: Weight of the next hop. The value range is from 1 to 8, and the default value is **1**.

interface *out-interface-type out-interface-number*: Output interface type and number of the next hop.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can specify multiple **ip policy-source in-interface** commands for the same interface. The sequence numbers of different source addresses must be different. A smaller sequence number indicates a higher priority of the source-address-based PBR.

If the sequence numbers are the same, the priorities of next hop types are as follows: **vrf** *vrf-name* > **next-hop** *ipv4-address* > **interface** *out-interface-type*> **default next-hop** *ipv4-address* > **default interface** *out-interface-type*.

The source-address-based PBR has a lower priority than the interface-based PBR. If the source-address-based PBR and the interface-based PBR are applied to the same interface, only the interface-based PBR takes effect.

Examples

The following example configures PBR for packets received by GigabitEthernet 0/0, sets the next hop of packets with the source address 10.0.0.2 to **196.168.1.2** and the next hop of packets with the source address 20.0.0.2 to **196.168.2.2**; otherwise, packets are normally forwarded.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip policy-source in-interface gigabitEthernet 0/0 1 10.0.0.2
255.255.255.255 next-hop 196.168.1.2
Hostname(config)# ip policy-source in-interface gigabitEthernet 0/0 2 20.0.0.2
255.255.255.255 next-hop 196.168.2.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ipv6 local policy route-map

Function

Run the **ipv6 local policy route-map** command to apply PBR to IPv6 packets sent by the local device.

Run the **no** form of this command to disable this feature.

By default, no IPv6 PBR is applied to the local device.

Syntax

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map

Parameter Description

route-map-name: Name of the route map applied to the local PBR. It is configured by the **route-map** command.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command enables PBR for only IPv6 packets (such as **ping** packets) that are sent by the local device and match the policy. It is not applicable to IPv6 packets received by the local device.

To apply PBR, you must specify a route map for PBR, and create this map. A route map consists of multiple policies, and one or more match rules and relevant actions are defined for each policy. After PBR is applied to an interface, all packets received by the interface are checked. Packets that do not match any policy in the route map are routed and forwarded as usual. Packets that match a policy in the route map are processed based on the action defined in the policy.

Examples

The following example applies PBR to a local device. Packets that are routed from 2003:1000::10/80 to 2001:100::/64 and match the ACL **aaa** are sent to the device 2003:1001::2.

(1) Configure the ACL **aaa** to match packets that are routed from 2003:1000::10/80 to 2001:100::/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list aaa
Hostname(config-ipv6-acl)# permit ipv6 2003:1000::10/80 2001:100::/64
Hostname(config-ipv6-acl )# exit
```

(2) Configure the route map **pbr-aaa**, and set the next hop of packets that match the ACL **aaa** to **2003:1001::2**.

```
Hostname(config)# route-map pbr-aaa permit 10
Hostname(config-route-map)# match ipv6 address aaa
Hostname(config-route-map)# set ipv6 next-hop 2003:1001::2
Hostname(config-route-map)# exit
```

(3) Apply PBR to the device.

```
Hostname(config)# ipv6 local policy route-map pbr-aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ipv6 policy

Function

Run the **ipv6 policy** command to configure redundant backup or load balancing among multiple next hops for PBR.

Run the **no** form of this command to restore the default configuration.

By default, multiple next hops of the IPv6 PBR adopt the redundant backup mode.

Syntax

ipv6 policy { load-balance | redundance }

no ipv6 policy

Parameter Description

load-balance: Adopts load balancing.

redundance: Adopts redundant backup.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **set ipv6 next-hop** command to configure multiple next hops. The next-hop selection policy configured by this command is redundant backup or load balancing. When redundant backup is configured, only the first parsed next hop of PBR takes effect. When load balancing is configured, multiple parsed next hops of PBR take effect. You can configure up to 8 next hops in the case of Weighted Cost Multiple Path (WCMP), or 32 next hops in the case of Equal Cost Multiple Path (ECMP).

Caution

The next hop refers to the next hop of which the MAC address is learned.

Examples

The following example configures the load balancing mode among multiple next hops.

(1) Configure ACL 1 to match the traffic from the IP address 1000::1, and ACL 2 to match the traffic from the IP address 2000::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list 1
```

```
Hostname(config-ipv6-acl )# permit ipv6 1000::1 any
Hostname(config-ipv6-acl )# exit
Hostname(config)# ipv6 access-list 2
Hostname(config-ipv6-acl )# permit ipv6 2000::1 any
Hostname(config-ipv6-acl )# exit
```

(2) Configure the sequence number 10 for the route map **lab1**, and set multiple next hops for traffic that matches ACL 1. Configure the sequence number 20 for the route map **lab1**, and set multiple next hops for traffic that matches ACL 1.

```
Hostname(config)# route-map lab1 permit 10
Hostname(config-route-map)# match ipv6 address 1
Hostname(config-route-map)# set ipv6 next-hop 2002::1
Hostname(config-route-map)# set ipv6 next-hop 2002::2
Hostname(config-route-map)# set ipv6 next-hop 2002::3
Hostname(config-route-map)# exit
Hostname(config)# route-map lab1 permit 20
Hostname(config-route-map)# match ipv6 address 2
Hostname(config-route-map)# set ipv6 next-hop 2002::5
Hostname(config-route-map)# set ipv6 next-hop 2002::6
Hostname(config-route-map)# set ipv6 next-hop 2002::7
Hostname(config-route-map)# exit
```

(3) Apply PBR to the interface.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if)# ipv6 policy route-map lab1
Hostname(config-if)# exit
Hostname(config)# ipv6 policy load-balance
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ipv6 policy route-map

Function

Run the **ipv6 policy route-map** command to apply the IPv6 PBR to an interface.

Run the **no** form of this command to remove this configuration.

By default, no IPv6 PBR is configured on an interface.

Syntax

ipv6 policy route-map *route-map-name*

no ipv6 policy route-map

Parameter Description

route-map-name: Name of the route map, which is configured by the **route-map** command.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The IPv6 PBR applied to an interface takes effect on only IPv6 packets received by this interface. You can configure only one IPv6 route map for an interface on a device. If you configure multiple route maps for the same interface, the latest route map overwrites the previous route maps.

To apply PBR, you must specify a route map for PBR, and create this map. A route map consists of multiple policies, and one or more match rules and relevant actions are defined for each policy. After PBR is applied to an interface, all packets received by the interface are checked. Packets that do not match any policy in the route map are routed and forwarded as usual. Packets that match a policy in the route map are processed based on the action defined in the policy.

Rules in the route map used for the IPv6 PBR must be supported by IPv6; otherwise, these rules do not take effect.

Examples

The following example configures PBR for IPv6 packets received by GigabitEthernet 0/0, sets the next hop of packets with the source address 10::/64 to **2000:1** and the next hop of packets with the source address 20::/64 to **2000::2**; otherwise, packets are normally forwarded.

(1) Configure the ACL **acl_for pbr1** to match the traffic from the source address 10::/64, and the ACL **acl_for_pbr2** to match the traffic from the source address 20::/64.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 access-list acl_for_pbr1
Hostname (config-ipv6-acl)# permit ipv6 10::/64  any
Hostname (config-ipv6-acl)# exit
Hostname(config)# ipv6 access-list acl_for_pbr2
Hostname (config-ipv6-acl)# permit ipv6 20::/64  any
Hostname (config-ipv6-acl)# exit
```

(2) Configure the sequence number 10 for the route map **rm_pbr**, and set the next hop of traffic that matches the ACL **acl_for_pbr1** to **2000::1**. Configure the sequence number 20 for the route map **rm_pbr** , and set the next hop of traffic that matches the ACL **acl_for_pbr2** to **2000::2**.

```
Hostname(config)# route-map rm_pbr  permit 10
Hostname (config-route-map)# match ipv6 address acl_for_pbr1
Hostname(config-route-map)# set ipv6 next-hop 2000::1
Hostname(config-route-map)# exit
Hostname(config)# route-map rm_pbr  permit 20
Hostname(config-route-map)# match ipv6 address acl_for_pbr2
Hostname(config-route-map)# set ipv6 next-hop 2000::2
Hostname(config-route-map)# exit
```

(3) Apply the route map to the interface.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if)# no switchport
Hostname(config-if)# ipv6 policy route-map rm_pbr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 policy-source in-interface

Function

Run the **ipv6 policy-source in-interface** command to apply source-address-based PBR to IPv6 packets received by a specified interface.

Run the **no** form of this command to remove this configuration.

By default, no source-address-based IPv6 PBR takes effect on an interface.

Syntax

ipv6 policy-source in-interface *interface-type interface-number sequence source-address/prefix-length* { [**default**] **next-hop** [*ipv6-address* [*weight*]]&<1-4> | [**default**] **interface** *out-interface-type*&<1-4> }

no ipv6 policy-source in-interface *interface-type sequence* [*source-address/prefix-length* [[**default**] **next-hop** [*ipv6-address* [*weight*]]&<1-4> | [**default**] **interface** *out-interface-type*&<1-4>]]

Parameter Description

interface-type interface-number: Type and number of the interface to which source-address-based PBR is applied.

sequence: Sequence number of a policy. A smaller sequence number indicates a higher priority.

source-address: IPv6 address.

prefix-length: Prefix length of the IPv6 address.

default: If this parameter is configured, the system preferentially uses the route forwarding table to forward packets; otherwise, the system preferentially uses PBR to forward packets.

next-hop [*ipv6-address* [*weight*]]&<1-4>: You can enter up to four next-hop IPv6 addresses and weight values.

ipv6-address: IPv6 address of the next hop.

weight: Weight of the next hop. The value range is from 1 to 8, and the default value is **1**.

interface *out-interface-type*: Output interface type of the next hop.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can specify multiple **ipv6 policy-source in-interface** commands for the same interface. The sequence numbers of different source addresses must be different. A smaller sequence number indicates a higher priority of the source-address-based PBR.

If the sequence numbers are the same, the priorities of next hop types are as follows: **vrf** *vrf-name* > **next-hop** *ipv6-address* > **interface** *out-interface-type*> **default next-hop** *ipv6-address* > **default interface** *out-interface-type*.

The source-address-based PBR has a lower priority than the interface-based PBR. If the source-address-based PBR and the interface-based PBR are applied to the same interface, only the interface-based PBR takes effect.

Examples

The following example configures PBR for IPv6 packets received by GigabitEthernet 0/0, sets the next hop of packets with the source address 10::/64 to **2000:1** and the next hop of packets with the source address 20::/64 to **2000::2**; otherwise, packets are normally forwarded.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 policy-source in-interface gigabitEthernet 0/0 2 10::/64 next-hop
2000::1
Hostname(config)# ipv6 policy-source in-interface gigabitEthernet 0/0 2 20::/64 next-hop
2000::2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show ip pbr bfd

Function

Run the **show ip pbr bfd** command to display the correlation between the IPv4 PBR and BFD.

Syntax

show ip pbr bfd

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the correlation between the IPv4 PBR and BFD.

Examples

The following example displays the correlation between the IPv4 PBR and BFD.

```
Hostname> enable
Hostname# show ip pbr bfd
VRF ID  Ifindex  Host           State  Refcnt
    0       13  192.168.8.100      Up       2
```

Table 1-1 Output Fields of the show ip pbr bfd Command

Field	Description
VRF ID	VRF of the interface carrying the BFD neighbor correlated with PBR
Ifindex	Index of the interface carrying the BFD neighbor correlated with PBR
Host	IPv4 address of the peer
State	Up or down state of the BFD neighbor correlated with PBR
Refcnt	Neighbor reference count

Notifications

N/A

Platform Description

N/A

1.12 show ip pbr route

Function

Run the **show ip pbr route** command to display the IPv4 PBR applied to an interface.

Syntax

show ip pbr route [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Displays the IPv4 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv4 PBR is applied are displayed.

local: Displays the IPv4 PBR applied to a local interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the PBR configured for an interface.

Examples

The following example displays the IPv4 PBR applied to an interface.

```
Hostname> enable
Hostname# show ip pbr route
PBR IPv4 Route Summay : 1
Interface       : GigabitEthernet 0/1
  Sequence      : 10
  ACL[0]       : 2900
ACL_CLS[0]    : 0
  Min Length    : None
  Max Length    : None
  VRF ID        : 0
  Route Flags   :
   Route Type   : PBR
   Direct       : Permit
   Priority     : High
   Tos_Dscp     : None
   Precedence   : None
  Tos_Dscp      : 0
  Precedence    : 0
  Mode          : redundance
  Nexthop Count  : 1
   Nexthop[0]   : 192.168.8.100
   Weight[0]    : 1
   Ifindex[0]   : 2
```

Table 1-2 Output Fields of the show ip pbr route Command

Field	Description
PBR IPv4 Route Summary	Number of IPv4 PBR entries.
Interface	Interface applying the PBR.
Sequence	Sequence number corresponding to the PBR.

Field	Description
ACL	ID of the ACL used in the matching rule.
ACL_CLS	Type of the ACL used in the matching rule, for example, the IP standard ACL.
Min Length	Minimum packet length set in the matching length
Max Length	Maximum packet length set in the matching length.
VRF ID	ID of the VRF correlated with the interface.
Route Flags	PBR flag.
Route Type	PBR type. The value **PBR** indicates a PBR route, and **Normal** indicates a common route.
Direct	PBR matching mode, which is **permit** or **deny**.
Priority	PBR priority, which is **High** or **Low**.
Tos_Dscp	Indicates whether to configure the ToS or DSCP rule.
Precedence	Indicates whether to configure the set ip precedence rule.
Mode	Configures the redundant backup or load balancing mode for the next hop.
Nexthop Count	Configures the number of next hops. Up to 32 next hops are configured for ECMP.
Nexthop	Configures the IPv4 address of the next hop.
Weight	Configures the weight value of the next hop.
Ifindex	Configures the index of the output interface corresponding to the next hop.

Notifications

N/A

Platform Description

N/A

1.13 show ip pbr route-map

Function

Run the **show ip pbr route-map** command to display the route map information of IPv4 PBR.

Syntax

show ip pbr route-map *route-map-name*

Parameter Description

route-map-name: Name of the route map, which is configured by the **route-map** command.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the route map information of IPv4 PBR.

Examples

The following example displays the route map information of IPv4 PBR.

```
Hostname> enable
Hostname# show ip pbr route-map rm
Pbr VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

route-map rm
  route-map index: sequence 10, permit
    Match rule:
      ACL ID :     0, ACL CLS: 0, Name: acl1
    Set rule:
      IPv4 Nexthop: 192.168.8.100, (VRF Name: , ID: 0), Weight: 0
      PBR state info ifx: GigabitEthernet 0/1, Connected: True, Track State: Up
```

Table 1-3 Output Fields of the show ip pbr route-map rm Command

Field	Description
Pbr VRF	Name and ID of the VRF.
Forward Mode	Configures the load balancing or redundant backup mode for the next hop.
Forwarding	Indicates whether to enable IP route forwarding.
Route-map index	Sequence number and type of the route submap.

Field	Description
Match rule	Matching rule.
Set rule	Set rule.
PBR state info	PBR private data, for example, the output interface and connection status of the next hop.

Notifications

N/A

Platform Description

N/A

1.14 show ip pbr source-route

Function

Run the **show ip pbr source-route** command to display the routing information of the source-address-based IPv4 PBR.

Syntax

show ip pbr source-route [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the IPv4 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv4 PBR is applied are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the configured source-address-based PBR.

Examples

The following example displays the routing information of the source-address-based IPv4 PBR.

```
Hostname> enable
Hostname# show ip pbr source-route
```

```
PBR IPv4 Source Route
Interface       : GigabitEthernet 0/1
  Sequence      : 10
  Source address : 10.1.1.1/24
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Match_ipaddr  : Exist
  Mode          : redundance
  Nexthop Count  : 1
   Nexthop[0]   : 192.168.8.100
   Weight[0]    : 1
   Ifindex[0]   : 2
```

Table 1-4 Output Fields of the show ip pbr source-route Command

Field	Description
Interface	Interface applying the PBR.
Sequence	Sequence number corresponding to the PBR.
VRF ID	ID of the VRF correlated with the interface.
Route Flags	PBR flag.
Route Type	PBR type. The value **PBR** indicates a PBR route, and **Normal** indicates a common route.
Direct	PBR matching mode, which is **permit** or **deny**.
Priority	PBR priority, which is **High** or **Low**.
Mode	Configures the redundant backup or load balancing mode for the next hop.
Nexthop Count	Configures the number of next hops. Up to 32 next hops are configured for ECMP.
Nexthop	Configures the IPv4 address of the next hop.
Weight	Configures the weight value of the next hop.
Ifindex	Configures the index of the output interface corresponding to the next hop.

Notifications

N/A

Platform Description

N/A

1.15 show ip pbr statistics

Function

Run the **show ip pbr statistics** command to display the statistics about packets forwarded by the IPv4 PBR.

Syntax

show ip pbr statistics [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Displays the IPv4 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv4 PBR is applied are displayed.

local: Displays the IPv4 PBR applied to a local interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the statistics about packets forwarded by the IPv4 PBR.

Examples

The following example displays the statistics about packets forwarded by the IPv4 PBR.

```
Hostname> enable
Hostname# show ip pbr statistics
IPv4 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 10
```

Table 1-5 Output Fields of the show ip pbr statistics Command

Field	Description
IPv4 Policy-based route statistic	Statistics about packets that match IPv4 PBR in the software
statistics	Interface statistics

Notifications

N/A

Platform Description

N/A

1.16 show ip policy

Function

Run the **show ip policy** command to display interfaces for which the PBR is configured and the name of the route map applied to each interface.

Syntax

show ip policy [*route-map-name*]

Parameter Description

route-map-name: The interfaces applying the route map specified by this parameter. If optional parameters are not specified, all interfaces configured with the PBR are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the PBR configured in the current system.

Examples

The following example displays all the interfaces for which the PBR is configured and the name of the route map applied to each interface.

```
Hostname> enable
```

```
Hostname# show ip policy
Banlance Mode: redundance
Interface            Route map
local               test
GigabitEthernet 0/0    test
```

Table 1-6 Output Fields of the show ip policy Command

Field	Description
Balance Mode:	Running mode among multiple next hops
Interface	Name of the interface
Route map	Name of the route map

Notifications

N/A

Platform Description

N/A

1.17 show ipv6 pbr bfd

Function

Run the **show IPv6 pbr bfd** command to display the correlation between the IPv6 PBR and BFD.

Syntax

show ipv6 pbr bfd

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the correlation between the IPv6 PBR and BFD.

Examples

The following example displays the correlation between the IPv6 PBR and BFD.

```
Hostname> enable
Hostname# show ipv6 pbr bfd
VRF ID  Ifindex  Host                                  State  Refcnt
    0       13  2000::2                                Up       1
```

Table 1-7 Output Fields of the show ipv6 pbr bfd Command

Field	Description
VRF ID	VRF of the interface carrying the BFD neighbor correlated with PBR
Ifindex	Index of the interface carrying the BFD neighbor correlated with PBR
Host	IPv6 address of the peer
State	Up or down state of the BFD neighbor correlated with PBR
Refcnt	Neighbor reference count

Notifications

N/A

Platform Description

N/A

1.18 show ipv6 pbr route

Function

Run the **show IPv6 pbr route** command to display the IPv6 PBR applied to an interface.

Syntax

show ipv6 pbr route [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Displays the IPv6 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv6 PBR is applied are displayed.

local: Displays the IPv6 PBR applied to a local interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the PBR configured for an interface.

Examples

The following example displays the IPv6 PBR applied to an interface.

```
Hostname> enable
Hostname# show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface       : GigabitEthernet 0/2
  Sequence      : 10
  ACL[0]       : 2901
ACL_CLS[0]    : 0
  Min Length    : None
  Max Length    : None
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Tos_Dscp     : None
   Precedence    : None
  Tos_Dscp      : 0
  Precedence    : 0
  Mode          : redundance
  Nexthop Count  : 1
   Nexthop[0]   : 10::1
   Weight[0]    : 1
   Ifindex[0]   : 3
```

Table 1-8 Output Fields of the show ipv6 pbr route Command

Field	Description
PBR IPv4 Route Summary	Number of IPv4 PBR entries.

Field	Description
Interface	Interface applying the PBR.
Sequence	Sequence number corresponding to the PBR.
ACL	ID of the ACL used in the matching rule.
ACL_CLS	Type of the ACL used in the matching rule, for example, the IP standard ACL.
Min Length	Minimum packet length set in the matching length.
Max Length	Maximum packet length set in the matching length.
VRF ID	ID of the VRF correlated with the interface.
Route Flags	PBR flag.
Route Type	PBR type. The value **PBR** indicates a PBR route, and **Normal** indicates a common route.
Direct	PBR matching mode, which is **permit** or **deny**.
Priority	PBR priority, which is **High** or **Low**.
Tos_Dscp	Indicates whether to configure the ToS or DSCP rule.
Precedence	Indicates whether to configure the set ip precedence rule.
Mode	Configures the redundant backup or load balancing mode for the next hop.
Nexthop Count	Configures the number of next hops. Up to 32 next hops are configured for ECMP.
Nexthop	Configures the IPv4 address of the next hop.
Weight	Configures the weight value of the next hop.
Ifindex	Configures the index of the output interface corresponding to the next hop.

Notifications

N/A

Platform Description

N/A

1.19 show ipv6 pbr route-map

Function

Run the **show IPv6 pbr route-map** command to display the route map information of IPv6 PBR.

Syntax

show ipv6 pbr route-map *route-map-name*

Parameter Description

route-map-name: Name of the route map, which is configured by the **route-map** command.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the route map information of IPv6 PBR.

Examples

The following example displays the route map information of IPv6 PBR.

```
Hostname> enable
Hostname# show ipv6 pbr route-map rm6
Pbr VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

route-map rm6
  route-map index: sequence 10, permit
Match rule:
  ACL ID :     0, ACL CLS: 0, Name: acl6
    Set rule:
      IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0
      PBR state info ifx: GigabitEthernet 0/0, Connected: True, Track State: Up
```

Table 1-9 show ipv6 pbr route-map rm6:

Field	Description
Pbr VRF	Name and ID of the VRF.

Field	Description
Forward Mode	Configures the load balancing or redundant backup mode for the next hop.
Forwarding	Indicates whether to enable IP route forwarding.
Route-map index	Sequence number and type of the route submap.
Match rule	Matching rule.
Set rule	Set rule.
PBR state info	PBR private data, for example, the output interface and connection status of the next hop.

Notifications

N/A

Platform Description

N/A

1.20 show ipv6 pbr source-route

Function

Run the **show ipv6 pbr source-route** command to display the routing information of the source-address-based IPv6 PBR.

Syntax

show ipv6 pbr source-route [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the IPv6 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv6 PBR is applied are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the configured source-address-based PBR.

Examples

The following example displays the routing information of the source-address-based IPv6 PBR.

```
Hostname> enable
Hostname# show ipv6 pbr source-route
PBR IPv6 Source Route
Interface       : GigabitEthernet 0/1
  Sequence      : 10
  Source address : 1000::1/64
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Match_ipaddr  : Exist
  Mode          : redundance
  Nexthop Count  : 1
   Nexthop[0]   : 1001::2
   Weight[0]    : 1
   Ifindex[0]   : 3
```

Table 1-10 Output Fields of the show ipv6 pbr source-route Command

Field	Description
Interface	Interface applying the PBR.
Sequence	Sequence number corresponding to the PBR.
VRF ID	ID of the VRF correlated with the interface.
Route Flags	PBR flag.
Route Type	PBR type. The value **PBR** indicates a PBR route, and **Normal** indicates a common route.
Direct	PBR matching mode, which is **permit** or **deny**.
Priority	PBR priority, which is **High** or **Low**.
Mode	Configures the redundant backup or load balancing mode for the next hop.
Nexthop Count	Configures the number of next hops. Up to 32 next hops are configured for ECMP.
Nexthop	Configures the IPv4 address of the next hop.
Weight	Configures the weight value of the next hop.

Field	Description
Ifindex	Configures the index of the output interface corresponding to the next hop.

Notifications

N/A

Platform Description

N/A

1.21 show ipv6 pbr statistics

Function

Run the **show ipv6 pbr statistics** command to display the statistics about packets forwarded by the IPv6 PBR.

Syntax

show ipv6 pbr statistics [**interface** *interface-type interface-number* | **local**]

Parameter Description

interface *interface-type interface-number*: Displays the IPv4 PBR applied to the specified interface. If optional parameters are not specified, all interfaces to which the IPv4 PBR is applied are displayed.

local: Displays the IPv4 PBR applied to a local interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to verify the statistics about packets forwarded by the IPv6 PBR.

Examples

The following example displays the statistics about packets forwarded by the IPv6 PBR.

```
Hostname> enable
Hostname# show ipv6 pbr statistics
IPv6 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 20
```

Table 1-11 Output Fields of the show ipv6 pbr statistics Command

Field	Description
IPv6 Policy-based route statistic	Statistics about packets that match IPv6 PBR in the software
statistics	Interface statistics

Notifications

N/A

Platform Description

N/A

1.22 show ipv6 policy

Function

Run the **show IPv6 policy** command to display interfaces for which the IPv6 PBR is configured and the name of the route map applied to each interface.

Syntax

show ipv6 policy [*route-map-name*]

Parameter Description

route-map-name: Name of the route map used for PBR.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run this command to check the layer-3 interfaces that apply the IPv6 PBR in the current system.

Examples

The following example displays all the interfaces for which the IPv6 PBR is configured and the name of the route map applied to each interface.

```
Hostname> enable
Hostname# show ipv6 policy
```

```
Banlance Mode: redundance
Interface            Route map
VLAN 1               RM_for_Vlan_1
VLAN 2               RM_for_Vlan_2
```

Table 1-12 Output Fields of the show ipv6 policy Command

Field	Description
Balance Mode	Running mode of the PBR on the current device
Interface	Interface applying the PBR
Route map	Name of the route map applied to the interface.

Notifications

N/A

Platform Description

N/A

1 Key Commands

Command	Function
accept-lifetime	Configure the accept-lifetime.
key	Configure a key in the key chain.
key chain	Configure a key chain, and enter the key chain configuration mode.
key-string	Configure a key string in the key configuration mode of the key chain.
send-lifetime	Configure the send-lifetime.
show key chain	Display the key chain configurations.

1.1 accept-lifetime

Function

Run the **accept-lifetime** command to configure the accept-lifetime.

Run the **no** form of this command to remove this configuration.

By default, the accept-lifetime of a key chain is disabled.

Syntax

accept-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

no accept-lifetime

Parameter Description

start-time: Start time of the lifetime.

infinite: Specifies that the key is always effective from the start time.

end-time: End time of the lifetime, which must be later than *start-time*.

duration *duration-time*: Specifies the duration of the lifetime starting from *start-time* in seconds. The range is from 1 to 2147483646.

Command Modes

Key configuration mode of the key chain

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the key chain **kc**, and enters the key chain configuration mode. The example also configures the key **1**, enters the key **1** configuration mode, and defines the accept-lifetime of the key chain.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# key chain kc
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string Hello
Hostname(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2010 duration 43200
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- key
- key chain

1.2 key

Function

Run the **key** command to configure a key in the key chain.

Run the **no** form of this command to remove this configuration.

By default, no key is configured.

Syntax

key *key-id*

no key *key-id*

Parameter Description

key-id: ID of the authentication key in the key chain. The value range is from 0 to 2147483647.

Command Modes

Key chain configuration mode.

Default Level

14

Usage Guidelines

After the key is configured, it must meet two conditions before it takes effect: (1) the key-string is configured; (2) the key is in the lifetime (send-lifetime and accept-lifetime). If the lifetime is not configured, the key is considered effective permanently once the key-string is configured. Two effective states are defined: effective on the sending end and effective on the receiving end. The two states correspond to send-lifetime and accept-lifetime respectively.

If there is no special demand, you can configure a key by incrementing the key-id to avoid the authentication state oscillation caused by the possible changes of effective keys. If multiple effective keys exist, each routing protocol uses the key with the smallest key-id.

In the TCP enhanced authentication scenario, the key-id ranges from 0 to 63.

Examples

The following example configures the key chain **ripkeys**, enters the key chain configuration mode, and configures the key **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# key chain ripkeys
Hostname(config-keychain)# key 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **key chain**
- **key-string**

1.3 key chain

Function

Run the **key chain** command to configure a key chain, and enter the key chain configuration mode.

Run the **no** form of this chain command to remove this configuration.

By default, no key chain is configured.

Syntax

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter Description

key-chain-name: Name of the key chain.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To make a key chain take effect, you must configure at least one key.

Examples

The following example configures the key chain **ripkeys**, and enters the key chain configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# key chain ripkeys
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **key**
- **key-string**

1.4 key-string

Function

Run the **key-string** command to configure a key string in the key configuration mode of the key chain.

Run the **no** form of this command to remove this configuration.

By default, no key string is configured.

Syntax

key-string [**0** | **7**] *string-text*

no key-string

Parameter Description

0: Specifies that the key is displayed in plaintext.

7: Specifies that the key is displayed in ciphertext.

string-text: key string. The plaintext key contains less than 80 characters; the ciphertext key contains less than 162 characters. The configured ciphertext parameter should be an even number of hexadecimal numbers (0-f). When the **service password-encryption** command is configured to enable the encryption service, the plaintext key is converted into a ciphertext key once the following condition is met: the ciphertext corresponding to the plaintext password is an even number of hexadecimal numbers and does not carry non-printable characters.

Command Modes

Key configuration mode of the key chain

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the key chain **ripkeys**, enters the key chain configuration mode, configures the key **1**, enters the key **1** configuration mode, and sets the key string to **abc**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# key chain ripkeys
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string abc
```

Notifications

When the configured plaintext key contains more than 80 characters or the ciphertext key contains more than 162 characters, the following error prompt will be displayed:

```
%Error: key string too long
```

When the configured ciphertext key such as **key-string 7 123** does not meet the encryption rule, the following error prompt will be displayed:

```
% Invalid encrypted password: 123
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **key**
- **key chain**

1.5 send-lifetime

Function

Run the **send-lifetime** command to configure the send-lifetime.

Run the **no** form of this command to remove this configuration.

By default, the send-lifetime of a key chain is disabled.

Syntax

send-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

no send-lifetime

Parameter Description

start-time: Start time of the lifetime.

infinite: Specifies that the key is always effective from the start time.

end-time: End time of the lifetime, which must be later than *start-time*.

duration *duration-time*: Specifies the duration of the lifetime starting from *start-time* in seconds. The value range is from 1 to 2147483646.

Command Modes

Key configuration mode of the key chain

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the key chain **kc**, enters the key chain configuration mode, configures the key **1**, enters the key **1** configuration mode, and sets the send-lifetime of the key chain to 43,200 seconds starting from 16:30:00 Oct 1 2010.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# key chain kc
Hostname(config-keychain)# key 1
Hostname(config-keychain-key)# key-string World
Hostname(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2010 duration 43200
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show key chain

Function

Run the **show key chain** command to display the key chain configurations.

Syntax

show key chain [*keychain-name*]

Parameter Description

keychain-name: Configurations of the specified key chain.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no key chain name is specified, the configurations of all key chains are displayed. Otherwise, only configurations of the specified key chain are displayed.

Examples

The following example displays the information of all key chains.

```
Hostname(config)#show key chain
key chain kc
   key 1 -- text "Hostname"
      accept-lifetime (12:11:00 May  2 2001) - (infinite)
      send-lifetime (always valid) - (always valid) [valid now]
```

Table 1-1 Output Fields of the show key chain Command

Field	Description
key chain	Name of the key chain
key	ID and string of the key
accept-lifetime	Lifetime of a key in the receiving direction
send-lifetime	Lifetime of a key in the sending direction

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

Multicast Commands

1. IPv4 Multicast Commands
2. IGMP Commands
3. PIM-SM Commands
4. PIM-DM Commands
5. IGMP Snooping Commands
6. MSDP Commands
7. IPv6 Multicast Commands
8. MLD Commands
9. PIM-SMv6 Commands
10. MLD Snooping Commands

1 IPv4 Multicast Route Management Commands

Command	Function
clear ip mroute	Clear IP multicast routing information.
clear ip mroute statistics	Clear statistics about the IP multicast routing information.
ip mroute	Configure a multicast static route.
ip multicast-routing	Enable the multicast routing function.
ip multicast boundary	Configure a multicast border for a specified group.
ip multicast route-limit	Configure the maximum number of entries for an IPv4 multicast routing table.
ip multicast rpf longest-match	Enable RPF route selection based on the longest match rule.
ip multicast static	Enable L2 direction control for multicast streams.
ip multicast ttl-threshold	Configure a time to live (TTL) threshold for an interface.
mc ref synchronize all	Restore a multicasting failure.
multicast ip-mac-mapping verification	Filter out multicast streams whose IP addresses do not match MAC addresses.
msf force-forwarding	Enable forced forwarding of multicast packets by software.
msf ipmc-overflow override	Enable the overwriting mechanism upon overflow of multicast hardware forwarding entries.
msf nsf	Configure multicast non-stop forwarding parameters.
show ip mrf mfc	Display forwarding entries of IPv4 multicast routes.
show ip mroute	Display information of a multicast forwarding entry.
show ip mroute count	Display count information of a multicast routing table.
show ip mroute dense	Display information of a multicast forwarding entry.
show ip mroute sparse	Display information of a multicast forwarding table.
show ip mroute static	Display IPv4 multicast static routes.
show ip mroute summary	Display information of a multicast forwarding entry.

show ip mvif	Display basic information of a multicast interface.
show ip rpf	Display the RPF information of a specified source address.
show msf msc	Display an IPv4 multi-layer multicast forwarding table.
show msf nsf	Display configuration of multicast non-stop forwarding.

1.1 clear ip mroute

Function

Run the **clear ip mroute** command to clear IP multicast routing information.

Syntax

clear ip mroute { * | *group-address* [*source-address*] }

Parameter Description

*: Clears all forwarding information in the multicast routing table.

group-address: Group address of a multicast route.

source-address: Source address of a multicast route.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear IP multicast routing information.

Examples

The following example clears IP multicast routing information of the group with address 230.0.0.1.

```
Hostname> enable
Hostname# clear ip mroute 230.0.0.1
```

Notifications

N/A

Platform Description

N/A

1.2 clear ip mroute statistics

Function

Run the **clear ip mroute statistics** command to clear statistics about the IP multicast routing information.

Syntax

clear ip mroute statistics { ***** | *group-address* [*source-address*] }

Parameter Description

*: Clears statistics about all the forwarding entries in the multicast routing table.

group-address: Group address of a multicast route.

source-address: Source address of a multicast route.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics about the multicast routing information of the group with address 230.0.0.1.

```
Hostname> enable
Hostname# clear ip mroute statistics 230.0.0.1
```

Notifications

N/A

Platform Description

N/A

1.3 ip mroute

Function

Run the **ip mroute** command to configure a multicast static route.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No multicast static route is configured by default.

Syntax

ip mroute *source-address mask* [**bgp** | **isis** | **ospf** | **rip** | **static**] { *rpf-addrress* | *interface-type interface-number* } [*distance*]

no ip mroute *source-address mask* [**bgp** | **isis** | **ospf** | **rip**]

default ip mroute *source-address mask* [**bgp** | **isis** | **ospf** | **rip**]

Parameter Description

source-address: Multicast source address.

mask: Mask of the multicast source address.

bgp: Uses the BGP protocol.

isis: Uses the IS-IS protocol.

ospf: Uses the OSPF protocol.

rip: Uses the RIP protocol.

static: Uses a static route.

rpf-address: Address of the reverse path forwarding (RPF) neighbor (next hop to the multicast source).

interface-type interface-number: RPF interface (outbound interface to the multicast source).

distance: Route administrative distance. The value range is from 0 to 255, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Multicast static routes are applicable only to RPF checking.

If an IP address of the outbound interface, other than that of the next hop, must be specified for a multicast static route, the outbound interface must be of the point-to-point type.

Examples

The following example configures a multicast static route and sets the address range of a source specific multicast (SSM) group to 232/8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

Notifications

If the number of multicast static routes on a device reaches the upper limit, the following notification will be displayed:

```
Exceeding maximum static multicast route limit.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip mroute static**

1.4 ip multicast-routing

Function

Run the **ip multicast-routing** command to enable the multicast routing function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The multicast routing function is disabled by default.

Syntax

ip multicast-routing

no ip multicast-routing

default ip multicast-routing

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The IPv4 multicast routing function must be enabled before an IPv4 multicast protocol is enabled.

Examples

The following example enables the multicast routing function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip multicast-routing
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip multicast boundary

Function

Run the **ip multicast boundary** command to configure a multicast border for a specified group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No multicast border is configured by default.

Syntax

ip multicast boundary *access-list* [**in** | **out**]

no ip multicast boundary *access-list* [**in** | **out**]

default ip multicast boundary *access-list* [**in** | **out**]

Parameter Description

access-list: Group address range defined by an ACL.

in: Indicates that a multicast border applies to the inbound direction of a multicast stream.

out: Indicates that a multicast border applies to the outbound direction of a multicast stream.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is executed, Internet Group Management Protocol (IGMP) and Protocol Independent Multicast Sparse Mode (PIM-SM) packets in the group range are filtered on this interface and multicast streams do not pass through this interface.

This command is associated with a standard access control list (ACL). If an extended ACL is used, an error occurs in filtering.

Examples

The following example configures SVI 1 as a border of all multicast groups.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard mul-boun
Hostname(config-std-nacl)# permit 233.3.3.0 0.0.0.255
Hostname(config-std-nacl)# exit
Hostname(config)# interface vlan 1
Hostname(config-if)# ip multicast boundary mul-boun
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip multicast route-limit

Function

Run the **ip multicast route-limit** command to configure the maximum number of entries for an IPv4 multicast routing table.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A maximum of 1000 entries can be added to an IPv4 multicast routing table by default.

Syntax

ip multicast route-limit *route-limit* [*max-threshold*]

no ip multicast route-limit

default ip multicast route-limit

Parameter Description

route-limit: Maximum number of multicast routes. The value range is from 1 to 64000.

max-threshold: Threshold number of multicast routes that triggers an alarm. The value range is from 1 to 64000, and the default value is **64000**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Due to limitations on hardware resources, routing entries that exceed the range permitted by hardware can be forwarded only by software, deteriorating the performance.

The configured value of *max-threshold* must be smaller than or equal to the value of *route-limit*.

Examples

The following example sets the maximum number of entries that can be added to an IPv4 multicast routing table to **500**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip multicast route-limit 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip mroute count**

1.7 ip multicast rpf longest-match

Function

Run the **ip multicast rpf longest-match** command to enable RPF route selection based on the longest match rule.

Run the **no** form match this command to disable this function.

Run the **default** form of this command to restore the default configuration.

A route with the highest priority is selected as the RPF route by default. If the priorities are consistent, a route is selected in the sequence of multicast static route, Multiprotocol Extensions for BGP (MBGP) route, and unicast route.

Syntax

ip multicast rpf longest-match

no ip multicast rpf longest-match

default ip multicast rpf longest-match

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The RPF route selection rules are as follows:

(1) Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table for RPF checking. Select one route out of the three optimal routes as the RPF route.

(2) If the command of RPF route selection based on the longest match rule is configured, the route with the longest match is selected out of the three optimal routes as the RPF route. If the three routes share the same subnet mask, the route with the highest priority is selected. If the priorities are consistent, a route is selected in the sequence of multicast static route, MBGP route, and unicast route.

(3) If the command of RPF route selection based on the longest match rule is not configured, the route with the highest priority is selected out of the three optimal routes. If the priorities are consistent, a route is selected in the sequence of multicast static route, MBGP route, and unicast route.

Examples

The following example enables RPF route selection based on the longest match rule.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip multicast rpf longest-match
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing**

1.8 ip multicast static

Function

Run the **ip multicast static** command to enable L2 direction control for multicast streams.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

No L2 direction control is enabled for a multicast stream by default.

Syntax

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

default ip multicast static *source-address group-address interface-type interface-number*

Parameter Description

source-address: Address of a multicast source.

group-address: Address of a multicast group.

interface-type interface-number: L2 interface that is allowed to forward this multicast stream.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can configure this command multiple times for a multicast stream. That is, configure multiple interfaces to forward the stream. After direction control is enabled for a multicast stream, this multicast stream can be forwarded only by these configured interfaces. Other interfaces are not allowed to forward the stream.

This command controls only the forwarding of multicast streams on interfaces, but does not directly affect the processing of protocol packets by the multicast protocols. However, some features of the multicast protocols (PIM-DM or PIM-SM) depend on the multicast streams. Behaviors of the multicast routing protocols may be affected.

Examples

The following example allows the multicast streams (192.168.43.4 and 225.1.1.5) to be forwarded from GigabitEthernet 0/1 and GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip multicast static 192.168.43.4 225.1.1.5 gigabitEthernet 0/1
Hostname(config)# ip multicast static 192.168.43.4 225.1.1.5 gigabitEthernet 0/2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip multicast ttl-threshold

Function

Run the **ip multicast ttl-threshold** command to configure a time to live (TTL) threshold for an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default TTL threshold for an interface is **0**.

Syntax

ip multicast ttl-threshold *ttl-threshold-value*

no ip multicast ttl-threshold

default ip multicast ttl-threshold

Parameter Description

ttl-threshold-value: TTL threshold for an interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

A device with multicast enabled can maintain a TTL threshold for each interface. Multicast packets whose TTL values are greater than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded. A TTL threshold takes effect only for multicast frames and must be configured on L3 interfaces.

Examples

The following example sets the TTL threshold for an interface to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip multicast ttl-threshold 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 mc ref synchronize all

Function

Run the **mc ref synchronize all** command to restore a multicasting failure.

Syntax

mc ref synchronize all

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the quantity of software entries is greater than the entry capacity supported by the hardware, and when the used entries drop below the hardware entry capacity, the entries that failed to be added cannot be automatically added again. You must manually run corresponding command to trigger entry adding. When an error occurs during multicasting, you can use this command to refresh the configuration.

Examples

The following example restores multicasting failure.

```
Hostname> enable
Hostname# mc ref synchronize all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 multicast ip-mac-mapping verification

Function

Run the **multicast ip-mac-mapping verification** command to filter out multicast streams whose IP addresses do not match MAC addresses.

Run the **no** form of this command to remove this configuration.

Multicast streams whose IP addresses do not match MAC addresses are not filtered out by default.

Syntax

multicast ip-mac-mapping verification

no multicast ip-mac-mapping verification

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is executed, if the IP addresses and MAC addresses in the header of packets do not match, corresponding multicast streams are filtered out.

Examples

The following example filters out multicast streams whose IP addresses do not match MAC addresses.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# multicast ip-mac-mapping verification
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 msf force-forwarding

Function

Run the **msf force-forwarding** command to enable forced forwarding of multicast packets by software.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The mechanism of forced forwarding of multicast packets by software is disabled by default.

Syntax

msf force-forwarding

no msf force-forwarding

default msf force-forwarding

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the mechanism of forced forwarding of multicast packets by software.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# msf force-forwarding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 msf ipmc-overflow override

Function

Run the **msf ipmc-overflow override** command to enable the overwriting mechanism upon overflow of multicast hardware forwarding entries.

Run the **no** form of this command to disable this function

Run the **default** form of this command to restore the default configuration.

The overwriting mechanism upon overflow of multicast hardware forwarding entries is disabled by default.

Syntax

msf ipmc-overflow override

no msf ipmc-overflow override

default msf ipmc-overflow override

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the overwriting mechanism upon overflow of multicast hardware forwarding entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# msf ipmc-overflow override
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 msf nsf

Function

Run the **msf nsf** command to configure multicast non-stop forwarding parameters.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum period for multicast protocol convergence is **20** seconds and the packet leakage time is **30** seconds by default.

Syntax

msf nsf { **convergence-time** *convergence-time* | **leak** *leak-time* }

no msf nsf { **convergence-time** | **leak** }

default msf nsf { **convergence-time** | **leak** }

Parameter Description

convergence-time *convergence-time*: Specifies the maximum period for multicast protocol convergence, in seconds. The value range is from 0 to 3600.

leak *leak-time*: Specifies the packet leakage time, in seconds. The value range is from 0 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum period for multicast protocol convergence to 300s and the packet leakage time to 200s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# msf nsf convergence-time 300
Hostname(config)# msf nsf leak 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show msf nsf**

1.15 show ip mrf mfc

Function

Run the **show ip mrf mfc** command to display forwarding entries of IPv4 multicast routes.

Syntax

show ip mrf mfc [*soure-address group-address*]

Parameter Description

source-address: Source address in the forwarding entry of a multicast route.

group-address: Group address in the forwarding entry of a multicast route.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The two parameters are optional, and the source address and group address must be specified simultaneously.

When no source address or group address is specified, all multicast forwarding cache (MFC) entries are displayed.

Examples

The following example displays all IPv4 multicast route forwarding entries whose source address is 20.0.1.30 and group address is 233.3.3.3.

```
Hostname> enable
Hostname# show ip mrf mfc 20.0.1.30 233.3.3.3
Multicast Routing and Forwarding Cache Table
(20.0.1.30, 233.3.3.3)
  FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
  Incoming interface: VLAN 1[4097]
  Outgoing interface list:
VLAN 3 (1)
```

Table 1-1 Output Fields of the show ip mrf mfc Command

Field	Description
FAST_SW	A flag indicating whether an entry allows quick forwarding. If non-Ethernet interface frame relay exists, no quick entry is generated.
SWTCHED	Specifies whether an entry is added to next-layer forwarding table.
MIN_MTU MTU	Minimum maximum transmission unit (MTU) value of an entry
MIN_MTU_IFINDEX	Index of an interface with the minimum MTU value
WRONG IF	Counts of multicast packets that come from an incorrect interface
Incoming interface	RPF inbound interface of an entry
VLAN 3 (1)	Specifies that the L3 outbound interface of an entry belongs to VLAN 3. The value 1 indicates the TTL threshold of this L3 interface.

Notifications

N/A

Platform Description

N/A

1.16 show ip mroute

Function

Run the **show ip mroute** command to display information of a multicast forwarding entry.

Syntax

show ip mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter Description

group-or-source-address: Group address or source address.

group-or-source-address: Group address or source address. The two addresses must be different.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of all multicast routing entries.

```
Hostname> enable
Hostname# show ip mroute
IP Multicast Routing Table
Flags: I – Immediate Stat, T – Timed Stat, F – Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: GigabitEthernet 2/1
Outgoing interface list:
GigabitEthernet 1/3
```

Table 1-2 Output Fields of the show ip mroute Command

Field	Description
Flags	● **I**: Makes statistics immediately. ● **T**: Scheduled statistics. ● **F**: Set to a forwarding table.
Timers: Uptime/Stat Expiry	Time at which this entry is created or ages
Interface State	Status of an interface
Owner	Owner of this entry, which may be a multicast routing protocol
Incoming interface	Expected inbound interface of a packet. If it is inconsistent with the actual inbound interface, the packet is discarded.
Outgoing interface list	List of outbound interfaces. Packets are forwarded out from the interfaces in the list.

Notifications

N/A

Platform Description

N/A

1.17 show ip mroute count

Function

Run the **show ip mroute count** command to display count information of a multicast routing table.

Syntax

show ip mroute count

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays count information of a routing table.

```
Hostname> enable
Hostname# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

Table 1-3 Output Fields of the show ip mroute count Command

Field	Description
Total x routes using y bytes memory	A total of x routes use y-byte memory.
Route limit/Route threshold	Maximum number of routes that can be added/threshold of routes
Total NOCACHE/WRONGmif/WHOLEPKT recv from fwd	Number of received packets that are unresolved/number of packets received from incorrect interfaces/number of well-known multicast packets
Total NOCACHE/WRONGmif/WHOLEPKT sent to clients	Number of unresolved packets sent to a client
Immediate/Timed stat updates sent to clients	Number of packets sent to a client and updated in time or number of packets sent to a client and updated as scheduled
Reg ACK recv/Reg NACK recv/Reg pkt sent	Number of received and confirmed register packets/number of received but unconfirmed register packets/number of register packets sent
Next stats poll	Next status update time
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts	Number of software forwarded packets: Number of packets/number of bytes Statistics of other packets: Number of packets sent from incorrect interfaces

Field	Description
Fwd msg counts: WRONGVIF/WHOLEPKT recv	Number of forwarded messages: Packets sent from incorrect interfaces/well-known multicast packets
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent	Number of client messages: Packets sent from incorrect interfaces/well-known multicast packets/packets updated in time/messages that are updated as scheduled
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent	Number of register packets: Number of received and confirmed register packets/number of received but unconfirmed register packets/number of register packets sent

Notifications

N/A

Platform Description

N/A

1.18 show ip mroute dense

Function

Run the **show ip mroute dense** command to display information of a multicast forwarding entry.

Syntax

show ip mroute dense

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of all multicast routing entries.

```
Hostname> enable
Hostname(config)# show ip mroute dense

IP Multicast Routing Table
```

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
```

Table 1-4 Output Fields of the show ip mroute dense Command

Field	Description
Flags	● **I**: Makes statistics immediately. ● **T**: Scheduled statistics. ● **F**: Set to a forwarding table.
Timers: Uptime/Stat Expiry	Time at which this entry is created or ages
Interface State	Status of an interface

Notifications

N/A

Platform Description

N/A

1.19 show ip mroute sparse

Function

Run the **show ip mroute sparse** command to display information of a multicast forwarding table.

Syntax

show ip mroute sparse

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of all multicast routing entries.

```
Hostname> enable
Hostname# show ip mroute sparse
```

```
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
```

Table 1-5 Output Fields of the show ipv6 mroute sparse Command

Field	Description
Flags	• **I**: Makes statistics immediately. • **T**: Scheduled statistics. • **F**: Set to a forwarding table.
Timers: Uptime/Stat Expiry	Time at which this entry is created or ages
Interface State	Status of an interface

Notifications

N/A

Platform Description

N/A

1.20 show ip mroute static

Function

Run the **show ip mroute static** command to display IPv4 multicast static routes.

Syntax

show ip mroute static

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Under the same conditions, a multicast static route has higher priority than a dynamic route learned.

Examples

The following example displays multicast static routes configured by users.

```
Hostname> enable
Hostname# show ip mroute static
Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13
  Protocol: , distance: 0
```

Table 1-6 Output Fields of the show ip mroute static Command

Field	Description
Mroute	Multicast route
RPF neighbor	RPF neighbor
Protocol	Protocol
distance	Administrative distance

Notifications

N/A

Platform Description

N/A

1.21 show ip mroute summary

Function

Run the **show ip mroute summary** command to display information of a multicast forwarding entry.

Syntax

show ip mroute summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays abstract information of routing entries.

```
Hostname> enable
```

```
Hostname# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: T
```

Table 1-7 Output Fields of the show ip mroute Command

Field	Description
Flags	• **I**: Makes statistics immediately. • **T**: Scheduled statistics. • **F**: Set to a forwarding table.
Timers: Uptime/Stat Expiry	Time at which this entry is created or ages
Interface State	Status of an interface

Notifications

N/A

Platform Description

N/A

1.22 show ip mvif

Function

Run the **show ip mvif** command to display basic information of a multicast interface.

Syntax

show ip mvif [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays basic information of the multicast interface that belongs to VLAN 1.

```
Hostname> enable
Hostname# show ip mvif vlan 1
Interface   Vif    Owner    TTL   Local        Remote     Uptime
          Idx    Module        Address      Address
VLAN 1     1     PIM-DM   2    192.168.1.1   0.0.0.0    00:13:16
```

Table 1-8 Output Fields of the show ip mvif Command

Field	Description
Interface	Interface
Vif Idx	Index of a multicast interface
Owner Module	Module name
TTL	Time to live
Local Address	Local address
Remote Address	Remote address of multicast virtual private network (VPN)
Uptime	Start time

Notifications

N/A

Platform Description

N/A

1.23 show ip rpf

Function

Run the **show ip rpf** command to display the RPF information of a specified source address.

Syntax

show ip rpf *source-address*

Parameter Description

source-address: Source address.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RPF information destined to 192.168.1.54.

```
Hostname# show ip rpf 192.168.1.54
RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

Table 1-9 Output Fields of the show ip rpf Command

Field	Description
RPF interface	RPF interface
RPF neighbor	RPF neighbor
RPF route	RPF route
RPF type	RPF type
RPF recursion count	RPF recursion count
Distance	Administrative distance
Metric	Measurement

Notifications

N/A

Platform Description

N/A

1.24 show msf msc

Function

Run the **show msf msc** command to display an IPv4 multi-layer multicast forwarding table.

Syntax

show msf msc [*soure-address*] [*group-address*] [*vlan-id*]

Parameter Description

soure-address: Source address in the multi-layer forwarding entry.

group-address: Group address in the multi-layer forwarding entry.

vlan-id: VLAN ID which an inbound interface belongs to in the multi-layer forwarding entry.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When only the source address is specified as S1, all MSC entries with the source address being S1 are displayed.

When the source address is specified as S1 and the group address is specified as G1, all MSC entries with the source address being S1 and the group address being G1 are displayed.

When the source address is specified as S1, the group address is specified as G1, and the VLAN ID is specified as V1, all MSC entries with the source address being S1, group address being G1, and the inbound interface belonging to V1 are displayed.

Examples

The following example displays the IPv4 multi-layer multicast forwarding entries with the source address being 192.168.195.25.

```
Hostname> enable
Hostname# show msf msc 192.168.195.25
Multicast Switching Cache Table
(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
  VLAN 1(0): 1 OPORTs, REQ: DONE
OPORT 6, IGMP-SNP, REQ: DONE
```

Table 1-10 Output Fields of the show msf msc Command

Field	Description
192.168.195.23	Source address in an entry
233.3.3.3	Group address in an entry
1	VLAN ID that an inbound interface of an entry belongs to
SYNC	Specifies that an entry has been synchronized to the bottom layer hardware.
MTU	MTU value of an entry
OIFs	Number of L3 outbound interfaces in an entry

Field	Description
VLAN1(0)	VLAN ID which L3 outbound interface OIFs belong to
1 OPORTs	Number of L2 interfaces belonging to the L3 outbound interface OIF
REQ: DONE	Specifies that this OIF has been set to the bottom layer hardware.
OPORT 6	L2 interfaces belonging to this OIF. The interfaces are indexed as 6.
IGMP-SNP	Specifies that this interface is created based on the IGMP Snooping protocol. **PIM-SNP**: This interface is created based on the PIM Snooping protocol. **ROUTER**: This interface is created based on the L3 protocol.
REQ: DONE	Specifies that this interface has been set to the bottom layer hardware.

Notifications

N/A

Platform Description

N/A

1.25 show msf nsf

Function

Run the **show msf nsf** command to display configuration of multicast non-stop forwarding.

Syntax

show msf nsf

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

```
Hostname> enable
Hostname# show msf nsf
Multicast HA Parameters
--------------------
protocol convergence timeout              120 secs
flow leak interval                       20 secs
```

Table 1-11 Output Fields of the show msf nsf Command

Field	Description
protocol convergence timeout	Maximum period for multicast protocol convergence
flow leak interval	Packet leakage time

Notifications

N/A

Platform Description

N/A

1 IGMP Commands

Command	Function
clear ip igmp group	Clear dynamic group member records in the IGMP cache.
clear ip igmp interface	Clear all IGMP statistics and group member records on an interface.
ip igmp access-group	Specify groups that the hosts are allowed to join on the interface.
ip igmp immediate-leave group-list	Enable the fast leave function on an interface.
ip igmp join-group	Add an interface to a group.
ip igmp last-member-query-count	Configure the times for sending specific group query packets on an interface.
ip igmp last-member-query-interval	Configure the interval for sending specific group query packets on an interface.
ip igmp limit	Configure the maximum number of IGMP group member records.
ip igmp mroute-proxy	Enable the MRoute proxy function on an interface.
ip igmp proxy-service	Enable the proxy service function on an interface.
ip igmp query-interval	Configure an interval for querying common group members.
ip igmp query-max-response-time	Configure the maximum response time for Query packets on an interface.
ip igmp query-timeout	Configure the survival period of other querier on an interface.
ip igmp robustness-variable	Configure the querier robustness variable on an interface.
ip igmp ssm-map enable	Enable the IGMP SSM mapping function.
ip igmp ssm-map static	Configure static mapping entries.
ip igmp static-group	Add a static interface to a group.
ip igmp version	Configure the IGMP version on an interface.

ip igmp enforce-router-alert	Enable the function of checking the Router Alert option in an IGMP packet and discarding an IGMP packet that does not carry the Router Alert option.
ip igmp enforce-source-subnet	Enable the source address checking function for IGMP Report packets.
ip igmp send-router-alert	Enable the function of containing the Router Alert option in an IGMP packet to be sent.
show ip igmp groups	Display groups directly connected to a device and group information learned from IGMP.
show ip igmp interface	Display configurations of an interface.
show ip igmp ssm-mapping	Display IGMP SSM mapping information.

1.1 clear ip igmp group

Function

Run the **clear ip igmp group** command to clear dynamic group member records in the IGMP cache.

Syntax

clear ip igmp group [*group-address* [*interface-type interface-number*]]

Parameter Description

group-address: Address of a group.

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The IGMP cache contains a list, which includes multicast groups to which hosts directly connected to a subnet are added. If a device is added to a multicast group, this group is included in this list as well.

If no parameter is specified in the command, all dynamic group member records are cleared from the IGMP cache.

Examples

The following example clears dynamic group member records in the IGMP cache.

```
Hostname> enable
Hostname# clear ip igmp group
```

Notifications

N/A

Platform Description

N/A

1.2 clear ip igmp interface

Function

Run the **clear ip igmp interface** command to clear all IGMP statistics and group member records on an interface.

Syntax

clear ip igmp interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear all IGMP learned group information and packet statistics on an interface. The packet statistics include received Report packets, Leave packets, and group member records on the current interface.

Examples

The following example clears all IGMP statistics and group member records on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ip igmp interface GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

1.3 ip igmp access-group

Function

Run the **ip igmp access-group** command to specify groups that the hosts are allowed to join on the interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Hosts can join any group by default.

Syntax

ip igmp access-group { *acl-name* | *acl-number* }

no ip igmp access-group

default ip igmp access-group

Parameter Description

acl-name: Name of a standard IP ACL that hosts can join. The value is a case-sensitive string of 1 to 99 characters.

acl- number: No. of a standard IP ACL that hosts can join. The value range is from 1 to 199 or from 1300 to 2699.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run this command on an interface to specify groups that you want hosts directly connected to a network segment to join. ACLs are used to limit the group address range. Report packets from groups denied by the ACLs are discarded.

When IGMPv3 is enabled, this command supports extended ACLs. When a received IGMP Report packet is (S1, S2, S3 … Sn, G), this command uses corresponding ACL to match (*,G). Therefore, to normally use this command, you must explicitly configure a (*,G) in the extended ACLs to filter (S1, S2, S3 … Sn, G).

Examples

The following example allows hosts on GigabitEthernet 0/1 to join only the group with the address 225.2.2.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp access-group 1
```

The following example associates a group list with extended ACLs on GigabitEthernet 0/1 to allow the interface to process IGMP packets with the source address 1.1.1.1 and group address 233.3.3.3.

```
Hostname# configure terminal
Hostname(config)# ip access-list extended ext_acl
Hostname(config-ext-nacl)# permit ip host 1.1.1.1 host 233.3.3.3
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp access-group ext_acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip igmp immediate-leave group-list

Function

Run the **ip igmp immediate-leave group-list** command to enable the fast leave function on an interface.

Run the **no** form of this command to disable this function on the interface.

Run the **default** form of this command to restore the default configuration.

The fast leave function on an interface is disabled by default.

Syntax

ip igmp immediate-leave group-list { *acl-name* | *acl-number* }

no ip igmp immediate-leave

default ip igmp immediate-leave

Parameter Description

acl-name: Name of a standard IP ACL. The value is a case-sensitive string of 1 to 99 characters.

acl- number: No. of a standard IP ACL. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command applies to an interface that runs IGMPv2 or IGMPv3 and that is connected to only one host.

After the fast leave function is enabled, if a device receives an IGMP Leave packet of a specified group, the device directly deletes this interface from the group member records to shorten the leave latency.

Examples

The following example enables the fast leave function on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 225.192.20.0 0.0.0.255
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp immediate-leave group-list 1
```

Notifications

If no access list exists, the following notification will be displayed:

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip igmp join-group

Function

Run the **ip igmp join-group** command to add an interface to a group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is added to a group by default.

Syntax

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

default ip igmp join-group *group-address*

Parameter Description

group-address: Address of a group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is run, the interface will simulate host behaviors and send a Join packet to the upstream device to join the specified group.

This command is used in lab test.

Examples

The following example adds GigabitEthernet 0/1 to the group with the address 233.3.3.3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp join-group 233.3.3.3
```

Notifications

If the group address is invalid, the following notification will be displayed:

```
Illegal multicast group address
```

If the interfaces in a group are full, the following notification will be displayed:

```
IGMP join-group limit reached
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip igmp last-member-query-count

Function

Run the **ip igmp last-member-query-count** command to configure the times for sending specific group query packets on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Specific group query packets are sent twice by default.

Syntax

ip igmp last-member-query-count *last-member-query-count-number*

no ip igmp last-member-query-count

default ip igmp last-member-query-count

Parameter Description

last-member-query-count-number: Times for sending specific group query packets. The value range is from 2 to 7.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command applies to IGMPv2 or IGMPv3 only.

After receiving a Leave packet through an interface, a multicast device continuously sends specific group query packets and waits for responses from the host. After timeout, the device considers that no group member exists in the directly-connected network segment and deletes this interface from the IGMP group member records. The timeout time is a product of the interval for sending specific group query packets and the times for sending the specific group query packets.

Examples

The following example sets the times for sending specific group query packets to 3 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp last-member-query-count 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.7 ip igmp last-member-query-interval

Function

Run the **ip igmp last-member-query-interval** command to configure the interval for sending specific group query packets on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The interval for sending specific group query packets is **1** second by default.

Syntax

ip igmp last-member-query-interval *last-member-query-interval*

no ip igmp last-member-query-interval

default ip igmp last-member-query-interval

Parameter Description

last-member-query-interval: Interval for sending specific group query packets, in 0.1 seconds. The value range is from 1 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command applies to IGMPv2 and IGMPv3 only.

After receiving a Leave packet through an interface, a multicast device continuously sends specific group query packets and waits for responses from the host. After timeout, the device considers that no group member exists in the directly-connected network segment and deletes this interface from the IGMP group member records. Timeout period = Interval for sending specific group query packets * Times for sending the specific group query packets

Examples

The following example sets the interval for sending specific group query packets to 20 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp last-member-query-interval 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.8 ip igmp limit

Function

Run the **ip igmp limit** command to configure the maximum number of IGMP group member records.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of IGMP group member records on an interface is **4000** by default. This number is **64000** in global configuration mode by default.

Syntax

ip igmp limit *limit-number* [**except** *acl-name* | **except** *acl-number*]

no ip igmp limit

default ip igmp limit

Parameter Description

limit *limit-number*: Specifies the maximum number of IGMP group member records. The value range is from 1 to 64000.

except *acl-name*: Specifies the name of a standard IP ACL. The groups in the ACL are not counted. The value is a case-sensitive string of 1 to 99 characters.

except *acl-number*: Specifies the No. of a standard IP ACL. The groups in the ACL are not counted. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

In global configuration mode, this command limits the number of IGMP group member records on a multicast device.

In interface configuration mode, this command limits the number of IGMP group member records on an interface.

If the number of group member records exceeds the interface limit or global limit, subsequent received Report packets are ignored.

If an except list is configured, Report packets in a specified range can be normally processed, but they are not counted.

Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, the global limit prevails.

Examples

The following example sets the maximum number of group members on GigabitEthernet 0/1 to 300, excluding the groups in the ACL1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp limit 300 except acl1
```

Notifications

If no access list exists, the following notification will be displayed:

```
% access-list acl1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.9 ip igmp mroute-proxy

Function

Run the **ip igmp mroute-proxy** command to enable the MRoute proxy function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.

The MRoute proxy function on an interface is disabled by default.

Syntax

ip igmp mroute-proxy *interface-type interface-number*

no ip igmp mroute-proxy

default ip igmp mroute-proxy

Parameter Description

interface-type interface-number: Type and number of a specified upstream interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp proxy-service** command to configure the upstream interface in the root direction of the multicast distribution tree as a proxy service interface.

You can run the **ip igmp mroute-proxy** command to configure the downstream interface in the leaf direction of the multicast distribution tree as an MRoute proxy interface.

The proxy service interface forwards an IGMP Query packet to the MRoute proxy interface. The MRoute proxy interface forwards an IGMP Report packet to the proxy service interface.

Examples

The following example enables the proxy service function on GigabitEthernet 0/1 and the MRoute proxy function on GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp proxy-service
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip igmp mroute-proxy GigabitEthernet 0/1
```

Notifications

If the multicast proxy function on an interface is disabled, the following notification will be displayed:

```
Mroute proxy had configured
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

- **show ip igmp interface**

1.10 ip igmp proxy-service

Function

Run the **ip igmp proxy-service** command to enable the proxy service function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.

The proxy service function on an interface is disabled by default.

Syntax

ip igmp proxy-service

no ip igmp proxy-service

default ip igmp proxy-service

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp proxy-service** command to configure the upstream interface in the root direction of the multicast distribution tree as a proxy service interface.

You can run the **ip igmp mroute-proxy** command to configure the downstream interface in the leaf direction of the multicast distribution tree as an MRoute proxy interface.

The proxy service interface forwards an IGMP Query packet to the MRoute proxy interface. The MRoute proxy interface forwards an IGMP Report packet to the proxy service interface.

A maximum of 32 proxy service interfaces can be configured on a device. After receiving an IGMP Query packet, the proxy service interface makes a response based on the IGMP group member records.

If the **switchport** command is executed on the proxy service interface, the **ip igmp mroute-proxy** command configured on the MRoute proxy interface is automatically deleted.

Examples

The following example enables the proxy service function on GigabitEthernet 0/1 and the MRoute proxy function on GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp proxy-service
```

```
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip igmp mroute-proxy GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)
- **show ip igmp interface**

1.11 ip igmp query-interval

Function

Run the **ip igmp query-interval** command to configure an interval for querying common group members.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default interval for querying common group members is **125** seconds.

Syntax

ip igmp query-interval

no ip igmp query-interval

default ip igmp query-interval

Parameter Description

query-interval: Interval for querying a common group member, in seconds. The value range is from 1 to 18000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for querying a common group member to 120 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp query-interval 120
```

Notifications

If the configured query interval is smaller than the maximum response time, the following notification will be displayed:

```
Query interval should be greater than Query Response Interval
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.12 ip igmp query-max-response-time

Function

Run the **ip igmp query-max-response-time** command to configure the maximum response time for Query packets on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum response time for query packets on an interface is **10** seconds by default.

Syntax

ip igmp query-max-response-time *query-max-response-time*

no ip igmp query-max-response-time

default ip igmp query-max-response-time

Parameter Description

query-max-response-time: Maximum response time, in seconds. The value range is from 1 to 25.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After sending Query packets, the interface waits for responses. After timeout, the interface considers that no group member exists in the directly-connected network segment and deletes the group information.

Examples

The following example sets the maximum response interval to 20 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp query-max-response-time 20
```

Notifications

If the configured maximum response time is greater than the query interval, the following notification will be displayed:

```
% Query Response Interval should be less than Query Interval
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.13 ip igmp query-timeout

Function

Run the **ip igmp query-timeout** command to configure the survival period of other querier on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The survival period of other querier is **255** seconds by default.

Syntax

ip igmp query-timeout *query-timeout*

no ip igmp query-timeout

default ip igmp query-timeout

Parameter Description

query-timeout: Survival period of other querier, in seconds. The value range is from 60 to 300.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After sending a Query packet, an interface waits for Query packets from other devices. After timeout, the device considers that it is the only querier on the directly-connected network segment.

Examples

The following example sets the survival period of other querier to 200 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp query-timeout 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.14 ip igmp robustness-variable

Function

Run the **ip igmp robustness-variable** command to configure the querier robustness variable on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default querier robustness variable is **2**.

Syntax

ip igmp robustness-variable *robustness-variable-number*

no ip igmp robustness-variable

default ip igmp robustness-variable

Parameter Description

robustness-variable-number: Querier robustness variable. The value range is from 2 to 7.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The querier robustness variable is used to calculate the aging time of a forwarding entry after a device receives an IGMP Report packet. Aging time = Query interval × Robustness variable + 10

Examples

The following example sets the querier robustness variable to 3 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp robustness-variable 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.15 ip igmp ssm-map enable

Function

Run the **ip igmp ssm-map enable** command to enable the IGMP SSM mapping function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The IGMP SSM mapping function is disabled by default.

Syntax

ip igmp ssm-map enable

no ip igmp ssm-map enable

default ip igmp ssm-map enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp ssm-map static** command to configure static mapping entries.

After this function is enabled, when an interface running IGMPv3 receives an IGMPv1 or IGMPv2 Report packet, the interface adds a static mapping source address.

Examples

The following example enables the IGMP SSM mapping function and sets the group mapping source address of ACL 11 to 192.168.2.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp ssm-map enable
Hostname(config)# ip igmp ssm-map static 11 192.168.2.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim ssm** (PIM-SM)
- **ip igmp ssm-map static**
- **show ip igmp ssm-mapping**

1.16 ip igmp ssm-map static

Function

Run the **ip igmp ssm-map static** command to configure static mapping entries.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static mapping entry is configured by default.

Syntax

ip igmp ssm-map static { *acl-name* | *acl-number* } *source-address*

no ip igmp ssm-map static { *acl-name* | *acl-number* } *source-address*

default ip igmp ssm-map static { *acl-name* | *acl-number* } *source-address*

Parameter Description

acl-name: Name of a standard IP ACL. The value is a case-sensitive string of 1 to 99 characters.

acl- number: No. of a standard IP ACL. The value range is from 1 to 99 or from 1301 to 1999.

source-address: Source address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp ssm-map enable** command to enable the IGMP SSM mapping function.

You can run this command to configure a static mapping entry.

After a static mapping entry is configured, when an interface running IGMPv3 receives an IGMPv1 or IGMPv2 Report packet, the interface adds a static mapping source address.

Examples

The following example enables the IGMP SSM mapping function and sets the group mapping source address of ACL 11 to 192.168.2.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp ssm-map enable
Hostname(config)# ip igmp ssm-map static 11 192.168.2.2
```

Notifications

If *source-address* is not a unicast address, the following notification will be displayed:

```
% Invalid input, not a unicast IP address 224.1.1.1!
```

If an inexistent ACL is applied, the following notification will be displayed:

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim ssm** (PIM-SM)
- **ip igmp ssm-map enable**
- **show ip igmp ssm-mapping**

1.17 ip igmp static-group

Function

Run the **ip igmp static-group** command to add a static interface to a group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static interface is added to a group by default.

Syntax

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

default ip igmp static-group *group-address*

Parameter Description

group-address: Address of a group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command adds an interface to a group without IGMP packet exchange. Even if no host exists in the group that resides on the same network segment as the interface, this interface is added to the group member records.

The record generated by adding a static interface to a group can be removed by using the **no ip igmp static-group** command, other than the **clear ip igmp group** command.

Examples

The following example adds GigabitEthernet 0/1 to the group with the address 236.6.6.6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp static-group 236.6.6.6
```

Notifications

If the group address is not an address of a multicast group, the following notification will be displayed:

```
Not a IP multicast group address
```

If the multicast group is full, the following notification will be displayed:

```
IGMP static-group limit reached
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.18 ip igmp version

Function

Run the **ip igmp version** command to configure the IGMP version on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

IGMPv2 runs on an interface by default.

Syntax

ip igmp version { **1** | **2** | **3** }

no ip igmp version

default ip igmp version

Parameter Description

1: Indicates IGMPv1.

2: Indicates IGMPv2.

3: Indicates IGMPv3.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is executed, the IGMP function automatically restarts.

Examples

The following example configures IGMPv3 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip igmp version 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp interface**

1.19 ip igmp enforce-router-alert

Function

Run the **ip igmp enforce-router-alert** command to enable the function of checking the Router Alert option in an IGMP packet and discarding an IGMP packet that does not carry the Router Alert option.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The function of checking the Router Alert option in an IGMP packet is disabled by default.

Syntax

ip igmp enforce-router-alert

no ip igmp enfore-router-alert

default ip igmp enfore-router-alert

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp enforce-router-alert** command to enable the Router Alert option checking function.

You can run the **no** form of this command to disable the Router Alert option checking function.

Examples

The following example enables the function of checking the Router Alert option in IGMP packets and discarding the IGMP packets that do not carry the Router Alert option.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp enforce-router-alert
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip igmp enforce-source-subnet

Function

Run the **ip igmp enforce-source-subnet** command to enable the source address checking function for IGMP Report packets.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The source address checking function for IGMP Report packets is disabled by default.

Syntax

ip igmp enforce-source-subnet

no ip igmp enforce-source-subnet

default ip igmp enforce-source-subnet

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp enforce-source-subnet** command to enable the source address checking function for IGMP Report packets. Only IGMP Report packets whose source addresses are on the same network segment as the packet receiving interface are received.

You can run the **no** form of this command to disable the source address checking function for IGMP Report packets.

If the source address in an IGMP Report packet is on the same network segment as the packet receiving interface, the packet can be received and the packet sending host can join the local group. If the source address in an IGMP Report packet is not on the same network segment as the packet receiving interface, the packet is rejected and the packet sending host cannot join the local group.

Examples

The following example enables source address checking for IGMP Report packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp enforce-source-subnet
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip igmp send-router-alert

Function

Run the **ip igmp send-router-alert** command to enable the function of containing the Router Alert option in an IGMP packet to be sent.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The Router Alert option is not contained in an IGMP packet to be sent by default.

Syntax

ip igmp send-router-alert

no ip igmp send-router-alert

default ip igmp send-router-alert

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run the **ip igmp send-router-alert** command to enable the function of containing the Router Alert option in an IGMP packet to be sent.

You can run the **no** form of this command to disable the function of containing the Router Alert option in an IGMP packet to be sent.

Examples

The following example enables the function of containing the Router Alert option in an IGMP packet to be sent.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp send-router-alert
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show ip igmp groups

Function

Run the **show ip igmp groups** command to display groups directly connected to a device and group information learned from IGMP.

Syntax

show ip igmp groups [*interface-type interface-number*] [*group-address*] [**detail**]

Parameter Description

group-address: Address of a group.

interface-type interface-number: Interface type and interface number.

detail: Displays detailed information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified in the command, the group addresses, interface types, and all multicast groups directly connected to the interfaces are displayed.

Examples

The following example displays all group information.

```
Hostname> enable
Hostname# show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires  Last Reporter
224.0.1.1       eth2  00:00:09  00:04:17  10.10.0.82
224.0.1.24      eth2  00:00:06  00:04:14  10.10.0.84
224.0.1.40      eth2  00:00:09  00:04:15  10.10.0.91
```

```
224.0.1.60      eth2  00:00:05  00:04:15  10.10.0.7
239.255.255.250 eth2  00:00:12  00:04:15  10.10.0.228
239.255.255.254 eth2  00:00:08  00:04:13  10.10.0.84
```

The following example displays detailed information of a group with the address 224.1.1.1.

```
Hostname> enable
Hostname# show ip igmp groups 224.1.1.1 detail
Interface: eth1
Group: 224.1.1.1
Uptime: 00:00:42
Group mode: Include
Last reporter: 192.168.50.111
TIB-A Count: 2
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)
Source Address Uptime v3 Exp Fwd Flags
192.168.55.55 00:00:42 00:03:38 Yes R
192.168.55.66 00:00:42 00:03:38 Yes R
```

Table 1-1 Output Fields of the show ip igmp groups Command

Field	Description
Group Address	Group address
Interface	Interface
Uptime	Update time
Expires	Remaining time
Last Reporter	Address of the last host that sends a Report packet
TIB-A Count	Number of source nodes in INCLUDE mode
TIB-B Count	Number of source nodes in EXCLUDE mode
Group source list	Linked list of source addresses
Source Address	Source address
Uptime	Source update time
v3 Exp	Source timeout time
Fwd Flags	Method of recording source addresses

Notifications

N/A

Platform Description

N/A

1.23 show ip igmp interface

Function

Run the **show ip igmp interface** command to display configurations of an interface.

Syntax

show ip igmp interface [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified in the command, configurations of all interfaces are displayed.

Examples

The following example displays configurations of all interfaces.

```
Hostname> enable
Hostname# show ip igmp interface
Interface vlan 1(Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
```

Table 1-2 Output Fields of the show ip igmp interface Command

Field	Description
Interface	Interface description
IGMP Active	IGMP status of an interface
IGMP querying router is x	Address of an IGMP querier router
IGMP query interval is x seconds	IGMP query interval

Field	Description
IGMP querier timeout is x seconds	IGMP query timeout time
IGMP max query response time is x seconds	Maximum response time for IGMP query packets
Last member query response interval is x milliseconds	Interval for querying the last member
Group Membership interval is x seconds	Interval for sending group member relationship

Notifications

N/A

Platform Description

N/A

1.24 show ip igmp ssm-mapping

Function

Run the **show ip igmp ssm-mapping** command to display IGMP SSM mapping information.

Syntax

show ip igmp ssm-mapping [*group-address*]

Parameter Description

group-address: Address of a group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified in the command, all IGMP SSM mapping information is displayed.

Examples

The following example displays the IGMP SSM mapping information of a group with the address 233.3.3.3.

```
Hostname> enable
Hostname# show ip igmp ssm-mapping 233.3.3.3
Group address: 233.3.3.3
Database    : Static
Source list  : 192.3.3.3
           : 3.3.3.3
```

Table 1-3 Output Fields of the show ip igmp ssm-mapping Command

Field	Description
Group Address	Group address
Database	Data status
Source list	Linked list of source addresses

Notifications

N/A

Platform Description

N/A

1 PIM-SM Commands

Command	Function
clear ip pim sparse-mode bsr rp-set	Clear dynamic rendezvous point (RP) information.
clear ip pim sparse-mode track	Reset the statistics start time and clear the counter of the PIM packets.
ip pim accept-bsr list	Limit the BSR address range.
ip pim accept-crp-with-null-group	Enable the BSR to receive C-RP-ADV packets with Prefix-Count being 0.
ip pim accept-crp list	Limit the C-RP address range and the address range of the groups served by the C-RPs.
ip pim accept-register	Limit the (S, G) address range in the register messages.
ip pim bsr-border	Configure a BSR border.
ip pim bsr-candidate	Configure C-BSRs.
ip pim bfd	Configure PIM-BFD correlation.
ip pim dr-priority	Configure the DR priority.
ip pim ignore-rp-set-priority	Ignore RP priority for RP election.
ip pim jp-timer	Configure the join/prune packet sending interval.
ip pim neighbor-filter	Enable the neighbor filtering function.
ip pim neighbor-tracking	Enable the neighbor tracking function.
ip pim override-interval	Configure the prune override interval of an interface.
ip pim probe-interval	Configure the register-probe time.
ip pim propagation-delay	Configure the propagation delay of an interface.
ip pim query-interval	Configure the hello message sending interval.
ip pim register-checksum-wholepkt	Calculate the checksum of entire packets.
ip pim register-decapsulate-forward	Enable the function for the RP to decapsulate register messages and forward multicast packets in the messages.
ip pim register-rate-limit	Limit the sending rate of register messages.

ip pim register-rp-reachability	Enable the RP reachability checking function before a register message is sent.
ip pim register-source	Specify a source IP address in register messages.
ip pim register-suppression	Configure the register suppression time.
ip pim rp-address	Configure static RPs.
ip pim rp-candidate	Configure C-RPs.
ip pim rp-register-kat	Configure the (S, G) entry timeout period on the RP.
ip pim sparse-mode	Enable the PIM-SM function on an interface.
ip pim sparse-mode passive	Enable the PIM-SM passive mode on an interface.
ip pim sparse-mode subvlan	Enable the PIM-SM function for sub VLANs of a super VLAN interface.
ip pim spt-threshold	Enable the shortest path tree (SPT) switchover function.
ip pim ssm	Enable the SSM function and configure an SSM group address range.
ip pim triggered-hello-delay	Configure the hello message sending delay on an interface.
show ip pim sparse-mode bsr-router	Display BSR information.
show ip pim sparse-mode interface	Display PIM-SM information of an interface.
show ip pim sparse-mode local-members	Display local IGMP information of a PIM-SM interface.
show ip pim sparse-mode mroute	Display PIM-SM routing information.
show ip pim sparse-mode neighbor	Display neighbor information.
show ip pim sparse-mode nexthop	Display next hop information, including interface number, address, and metric value of a next hop.
show ip pim sparse-mode rp-hash	Display RP information corresponding to a multicast group address.
show ip pim sparse-mode rp mapping	Display all RPs and the groups served by the RPs on the local device.
show ip pim sparse-mode track	Display the number of PIM packets sent and received since the statistic start time.

1.1 clear ip pim sparse-mode bsr rp-set

Function

Run the **clear ip pim sparse-mode bsr rp-set** command to clear dynamic rendezvous point (RP) information.

Syntax

clear ip pim sparse-mode bsr rp-set *

Parameter Description

*: Clears all dynamic RP information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to refresh the RP-Set.

This command cannot clear static RPs.

Examples

The following example clears dynamic RP-Set information.

```
Hostname> enable
Hostname# clear ip pim sparse-mode bsr rp-set *
```

Notifications

After the RP-Set information is cleared, the following notification will be displayed:

```
RP is changed for group range 224.0.0.0/4.  Perform RP change handler
```

Platform Description

N/A

1.2 clear ip pim sparse-mode track

Function

Run the **clear ip pim sparse-mode track** command to reset the statistics start time and clear the counter of the PIM packets.

Syntax

clear ip pim sparse-mode track

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example resets the statistic start time and clears the counter of the PIM packets.

```
Hostname> enable
Hostname# clear ip pim sparse-mode track
```

Notifications

```
N/A
```

Platform Description

N/A

1.3 ip pim accept-bsr list

Function

Run the **ip pim accept-bsr list** command to limit the BSR address range.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The BSR address range is not limited by default.

Syntax

ip pim accept-bsr list { *acl-name* | *acl-number* }

no ip pim accept-bsr

default ip pim accept-bsr

Parameter Description

list *acl-name*: Uses a standard IP ACL name to limit the BSR address range. The value is a case-sensitive string of 1 to 99 characters.

list *acl-number*: Uses a standard IP ACL number to limit the BSR address range. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the PIM-SM device receives only BSMs sent by legitimate BSRs.

Examples

The following example receives BSMs sent by the legitimate BSRs determined by the access list 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Hostname(config)# ip pim accept-bsr list 1
```

Notifications

If no ACL is configured to limit the BSR address range, the following notification will be displayed:

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim bsr-candidate**

1.4 ip pim accept-crp-with-null-group

Function

Run the **ip pim accept-crp-with-null-group** command to enable the BSR to receive C-RP-ADV packets with Prefix-Count being 0.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.
The function for the BSR to receive C-RP-ADV packets with Prefix-Count being 0 is disabled by default.

Syntax

ip pim accept-crp-with-null-group

no ip pim accept-crp-with-null-group

default ip pim accept-crp-with-null-group

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can receive C-RP-ADV packets with Prefix-Count being 0. This C-RP can support all groups.

Examples

The following example enables the BSR to receive C-RP-ADV packets with Prefix-Count being 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim accept-crp-with-null-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip pim accept-crp list

Function

Run the **ip pim accept-crp list** command to limit the C-RP address range and the address range of the groups served by the C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The C-BSRs receive all external C-RP advertisement packets by default.

Syntax

ip pim accept-crp list { *acl-name* | *acl-number* }

no ip pim accept-crp

default ip pim accept-crp

Parameter Description

list *acl-name*: Uses an extended IP ACL name to limit the C-RP address range and the address range of the groups served by the C-RPs. The value is a case-sensitive string of 1 to 99 characters.

list *acl-number*: Uses an extended IP ACL number to limit the C-RP address range and the address range of the groups served by the C-RPs. The value range is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can limit the C-RP address range and the address range of the groups served by the C-RPs.

Examples

The following example sets the C-RP address range and the address range of the groups served by the C-RPs to extended ACL 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 100
Hostname(config-ext-nacl)# permit ip 192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255
Hostname(config-ext-nacl)# exit
Hostname(config)# ip pim accept-crp list 100
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim rp-candidate**

1.6 ip pim accept-register

Function

Run the **ip pim accept-register** command to limit the (S, G) address range in the register messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The (S, G) address range of register messages is not limited by default. The RP receives register messages with any (S, G) address.

Syntax

ip pim accept-register { **list** { *acl-name* | *acl-number* } | **route-map** *route-map-name* } *
no ip pim accept-register
default ip pim accept-register

Parameter Description

list *acl-name*: Uses an extended IP ACL name to limit the (S, G) address range. The value is a case-sensitive string of 1 to 99 characters.

list *acl-number*: Uses an extended IP ACL number to limit the (S, G) address range. The value range is from 100 to 199 or from 2000 to 2699.

route-map *route-map-name*: Uses a route map to limit the (S, G) address range.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be run on a static RP or C-RP to limit the (S, G) address range in register messages.

Examples

The following example sets the (S, G) address range in register messages to access list 100, the source address to 192.168.195.0 with reverse mask 0.0.0.255, and the multicast group address to 255.1.1.1 with reverse mask 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1
0.0.0.255
Hostname(config)# ip pim accept-register list 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip pim bsr-border

Function

Run the **ip pim bsr-border** command to configure a BSR border.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.
No BSR border is configured by default.

Syntax

ip pim bsr-border
no ip pim bsr-border
default ip pim bsr-border

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To limit BSM flooding, you can configure a BSR border on the interface. Then, this interface discards received BSMs without forwarding them.

Examples

The following example configures a BSR border of PIM on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim bsr-border
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast boundary** (IPv4 multicast route management)
- **show ip pim sparse-mode interface**

1.8 ip pim bsr-candidate

Function

Run the **ip pim bsr-candidate** command to configure C-BSRs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.
No C-BSR is configured by default.

Syntax

ip pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ip pim bsr-candidate

default ip pim bsr-candidate

Parameter Description

interface-type interface-number: Specified interface.

hash-mask-length: Length of a hash mask configured for the RP election mechanism. The value range is from 0 to 32, and the default value is **10**.

priority-value: C-BSR priority. The value range is from 0 to 255, and the default value is **64**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In a PIM-SM domain, a unique BSR must be available. The BSR collects and releases RP information. Multiple C-BSRs elect an acknowledged BSR based on BSMs. Before a BSR is elected, each C-BSR considers itself a BSR and periodically sends a BSM with the multicast address 224.0.0.13 in the PIM-SM domain. This message includes the address and priority of the BSR.

This command can be used to send a BSM to all PIM neighbors through the interface assigned to the BSR. Each neighbor compares the original BSR address with the address in the received BSM. If the received BSM indicates that the C-BSR of the received BSM boasts a higher priority or a larger IP address, the neighbor saves the address in the BSM as the BSR address and forwards the BSM. Otherwise, the neighbor discards the BSM.

A C-BSR considers itself the BSR until the C-BSR receives a BSM indicating a higher priority from another C-BSR.

Examples

The following example configures a C-BSR to send a BSM through GigabitEthernet 0/1, and sets the hash mask length for the RP election mechanism to **30** and the priority to **192**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim bsr-candidate GigabitEthernet 0/1 30 192
```

Notifications

If the current interface is not set to the SM mode, the following notification will be displayed:

```
Warning: PIMSM not configured on %s, BSR messages not originated.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip pim bfd

Function

Run the **ip pim bfd** command to configure PIM-BFD correlation.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Syntax

ip pim bfd

no ip pim bfd

default ip pim bfd

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Bidirectional forwarding detection (BFD) is used to quickly detect or monitor links or IP route forwarding connectivity in a network.

Based on the PIM-SM protocol, a designated router (DR) is defined. This DR is the unique role that forwards multicast data in a shared network.

Devices in the shared network exchange hello messages and elect a DR based on the hello messages. When the DR is faulty, a new round of DR election can be started only after the PIM neighbor ages. If this command is run, when the DR is faulty, this faulty DR can be detected and a new round of election can be started in milliseconds.

Examples

The following example configures PIM-BFD correlation on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname (config-if-GigabitEthernet 0/1)# ip pim bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim sparse-mode**
- **show bfd neighbors** (reliability/BFD)

1.10 ip pim dr-priority

Function

Run the **ip pim dr-priority** command to configure the DR priority.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default DR priority is **1**.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority

default ip pim dr-priority

Parameter Description

priority-value: DR priority. A larger value indicates a higher priority. The value range is from 0 to 4294967294.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If multiple devices in a LAN join DR election, the election result is subject to the priorities in hello messages. The device with the highest priority is elected as the DR. If the priorities in the hello messages are the same or the priority parameter is not set in the hello messages, the device with the largest IP address is elected as the DR.

Examples

The following example sets the DR priority to **10000** on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim dr-priority 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.11 ip pim ignore-rp-set-priority

Function

Run the **ip pim ignore-rp-set-priority** command to ignore RP priority for RP election.

Run the **no** form of this command to preferentially select the C-RP with a higher priority.

Run the **default** form of this command to restore the default configuration.
A C-RP with the highest priority is selected as the RP by default.

Syntax

ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority
default ip pim ignore-rp-set-priority

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures to ignore RP priority for RP election.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim ignore-rp-set-priority
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip pim jp-timer

Function

Run the **ip pim jp-timer** command to configure the join/prune packet sending interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The join/prune packet is sent at an interval of **60** seconds by default.

Syntax

ip pim jp-timer *interval*

no ip pim jp-timer

default ip pim jp-timer

Parameter Description

interval: Join/prune packet sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the join/prune packet sending interval to 50 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim jp-timer 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ip pim neighbor-filter

Function

Run the **ip pim neighbor-filter** command to enable the neighbor filtering function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor filtering function is disabled by default.

Syntax

ip pim neighbor-filter { *acl-name* | *acl-number* }

no ip pim neighbor-filter { *acl-name* | *acl-number* }

default ip pim neighbor-filter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Standard IP ACL name that is used to limit the address range of neighbors. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Standard IP ACL number that is used to limit the address range of neighbors. The value range is from 1 to 99.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The neighbor filtering function can strengthen PIM network security and limit the valid address range of neighbors. If a neighbor is filtered out based on an access filtering list, PIM-SM does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

Examples

The following example uses ACL 14 to filter out a neighbor with the IP address 192.168.1.5 and the mask 0.0.0.255 on GigabitEthernet 0/1. PIM-SM does not create peer relationship with the neighbor (192.168.1.5).

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# access-list 14 deny 192.168.1.5 0.0.0.255
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim neighbor-filter 14
Hostname(config-if-GigabitEthernet 0/1)# exit
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list 14 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.14 ip pim neighbor-tracking

Function

Run the **ip pim neighbor-tracking** command to enable the neighbor tracking function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor tracking function is disabled by default.

Syntax

ip pim neighbor-tracking

no ip pim neighbor-tracking

default ip pim neighbor-tracking

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the suppression capability of an interface is enabled, when a multicast device plans to send a join packet to an uplink multicast device but it receives a join packet sent from the neighbor to the uplink multicast device, this local multicast device suppresses its own join packet. If the suppression capability of the interface is disabled, the join packet can be sent. When the suppression capability of downlink hosts is disabled, an uplink device can

determine the number of the downlink hosts based on the quantity of received join packets. This is neighbor tracking.

Examples

The following example disables the suppression function on GigabitEthernet 0/1 to implement neighbor tracking.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim neighbor-tracking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ip pim override-interval

Function

Run the **ip pim override-interval** command to configure the prune override interval of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.
The default prune override interval is **2500** ms.

Syntax

ip pim override-interval *override-interval*

no ip pim override-interval

default ip pim override-interval

Parameter Description

override-interval: Prune override interval, in milliseconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the prune override interval to 3000 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim override-interval 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim propagation-delay**
- **show ip pim sparse-mode interface**

1.16 ip pim probe-interval

Function

Run the **ip pim probe-interval** command to configure the register-probe time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default register-probe time is **5** seconds.

Syntax

ip pim probe-interval *interval*

no ip pim probe-interval

default ip pim probe-interval

Parameter Description

interval: Register-probe interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The register-probe time refers to the time when the source DR is allowed to send null register messages to the RP before the register suppression timer times out.

The register-probe time cannot be greater than a half of the register suppression time. Otherwise, the configuration fails and an alarm is generated.

The sum of the three times register suppression time and the register-probe time does not exceed 65535. Otherwise, the configuration fails and an alarm is generated.

Examples

The following example sets the register-probe time to 6 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim probe-interval 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip pim propagation-delay

Function

Run the **ip pim propagation-delay** command to configure the propagation delay of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default propagation delay of an interface is **500** ms.

Syntax

ip pim propagation-delay *propagation-delay*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description

propagation-delay: Propagation delay, in milliseconds. The value range is from 1 to 32767.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or override delay affects the prune override interval.

The network administrator must ensure that the override interval is smaller than the prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the override delay to 600 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim propagation-delay 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim override-interval**
- **show ip pim sparse-mode interface**

1.18 ip pim query-interval

Function

Run the **ip pim query-interval** command to configure the hello message sending interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The hello message is sent at an interval of **30** seconds by default.

Syntax

ip pim query-interval *interval*

no ip pim query-interval

default ip pim query-interval

Parameter Description

interval: Hello message sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the hello message sending interval is updated, the hello message hold time is updated accordingly. The hello message hold time is 3.5 times the hello message sending interval. If the product of the hello message sending interval and 3.5 is greater than 65535, the hello message sending interval is forcibly reset to 18725.

Examples

The following example sets the hello message sending interval to 123 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim query-interval 123
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.19 ip pim register-checksum-wholepkt

Function

Run the **ip pim register-checksum-wholepkt** command to calculate the checksum of entire packets.

Run the **no** form of this command to remove this configuration and calculate the checksum of headers of PIM packets and register messages, rather than the entire packets.

Run the **default** form of this command to restore the default configuration.

By default, only the headers of PIM packets and register messages, rather than the entire packets, are specified for calculating the checksum.

Syntax

ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

no ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

default ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

Parameter Description

group-list *acl-name*: Uses a standard IP ACL name to limit the addresses of multicast groups that support this configuration. The value is a case-sensitive string of 1 to 99 characters.

group-list *acl-number*: Uses a standard IP ACL number to limit the addresses of multicast groups that support this configuration. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The checksum of the entire PIM protocol packets (including encapsulated multicast packets), rather than the PIM headers of separate register messages, is calculated.

If the **group-list** parameter is not specified, the entire packet checksum calculation method applies to register messages with any group address.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits of the ACL associated with the **group-list** parameter are removed. In this case, the entire packet checksum calculation method applies to register messages with any group address.

Examples

The following example calculates the checksum of the entire packets whose multicast group addresses comply with ACL 99, where the multicast group address is 225.1.1.1 and the reverse mask is 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 99 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim register-checksum-wholepkt group-list 99
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list 99 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip pim register-decapsulate-forward

Function

Run the **ip pim register-decapsulate-forward** command to enable the function for the RP to decapsulate register messages and forward multicast packets in the messages.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function for the RP to decapsulate register messages and forward multicast packets in the messages is disabled by default.

Syntax

ip pim register-decapsulate-forward

no ip pim register-decapsulate-forward

default ip pim register-decapsulate-forward

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is run on a static RP or C-RP to decapsulate the received register messages and forward the multicast packets in the received register messages.

The register message decapsulation and multicast packet forwarding function is implemented by this command. If there are too many register messages to be decapsulated and forwarded, the CPU is overloaded. Therefore, you are not advised to enable this function.

Examples

The following example decapsulates the received register messages and forwards the multicast packets in the received register messages on the RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim register-decapsulate-forward
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip pim register-rate-limit

Function

Run the **ip pim register-rate-limit** command to limit the sending rate of register messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The sending rate of register messages is not limited by default.

Syntax

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

default ip pim register-rate-limit

Parameter Description

rate: Maximum number of register messages that can be sent per second. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the sending rate of register messages in (S, G) status, rather than that of the entire system. Running this command can reduce the load of the source DR and RP. Register messages sent at a rate exceeding the limit are discarded.

Examples

The following example sets the sending rate of register messages to 3000 per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim register-rate-limit 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip pim register-rp-reachability

Function

Run the **ip pim register-rp-reachability** command to enable the RP reachability checking function before a register message is sent.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The RP reachability checking function is disabled by default before a register message is sent.

Syntax

ip pim register-rp-reachability

no ip pim register-rp-reachability

default ip pim register-rp-reachability

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the RP reachability is checked before a register message is sent. If the RP is reachable, the message is sent. Otherwise, the message is not sent.

Examples

The following example enables the RP reachability checking function before a register message is sent.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim register-rp-reachability
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ip pim register-source

Function

Run the **ip pim register-source** command to specify a source IP address in register messages.

Run the **no** form of this command to specify the address of the DR interface connected to the source as the source IP address of register messages.

Run the **default** form of this command to restore the default configuration.

The source IP address in the register messages is the address of the DR interface connected to the source by default.

Syntax

ip pim register-source { *local-address* | *interface-type interface-number* }
no ip pim register-source
default ip pim register-source

Parameter Description

local-address: Source IP address in register messages.

interface-type interface-number: IP address of local interface, which is specified as source IP address of register messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configured source address in register messages must be reachable so that the source can react properly when the RP sends a correct register-stop message.

It is recommended that the loopback address be used as the source IP address in register messages. Other physical addresses can be used as the source IP addresses in register messages as well.

The status of the PIM function does not affect this configuration.

Examples

The following example specifies the IP address 192.168.195.80 of GigabitEthernet 0/1 as the source IP address in register messages.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ip pim register-source 192.168.195.80
Hostname(config)# ip pim register-source GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ip pim register-suppression

Function

Run the **ip pim register-suppression** command to configure the register suppression time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.
The default register suppression time is **60** seconds.

Syntax

ip pim register-suppression *suppression-time*

no ip pim register-suppression

default ip pim register-suppression

Parameter Description

suppression-time: Register suppression time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be run on the DR to configure the register suppression time.

If the **ip pim rp-register-kat** command is not run on the DR, configuring the register suppression time on the RP changes the RP keep-alive time.

Examples

The following example sets the register suppression time to 100 seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip pim register-suppression 100
```

Notifications

If two times the register-probe time is greater than the register suppression time, the following notification will be displayed:

```
WARNING: Register suppression interval MUST be larger than twice the register
probe interval. Please set a larger one.
```

If the sum of three times register suppression time and the register-probe time is greater than 65535, the following notification will be displayed:

```
WARNING: Register suppression interval is too large. It may cause (3*RST+probe-
interval) > 65535.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ip pim rp-address

Function

Run the **ip pim rp-address** command to configure static RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static RP is configured by default.

Syntax

ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

no ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

default ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

Parameter Description

rp-address: IP address of an RP.

acl-name: Standard IP ACL name that is used to limit the address range of groups served by this RP. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Standard IP ACL number that is used to limit the address range of groups served by this RP. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If static and dynamic RPs are available at the same time, dynamic RPs are preferred.

If multiple static RPs serve the same multicast group, the static RP with a larger address is preferred.

If the *acl-name* or *acl-number* parameter is not specified, the static RPs serve all groups.

Examples

The following example sets the IP address of a static RP to 210.34.0.55, the address of the group served by this RP to 255.1.1.1 (defined based on access list 4), and the reverse mask to 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 4 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim rp-address 210.34.0.55 4
```

Notifications

If the RP address is not a valid address, the following notification will be displayed:

```
Illegal RP address, ignored
```

If the number of RP addresses reaches the upper limit, the following notification will be displayed:

```
Reach PIM-SM static RP configuration limit 65536
```

If no ACL is configured, the following notification will be displayed:

```
% access-list 4 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode rp-hash**
- **show ip pim sparse-mode rp mapping**

1.26 ip pim rp-candidate

Function

Run the **ip pim rp-candidate** command to configure C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No C-RP is configured by default.

Syntax

ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval*] [**group-list** { *acl-name* | *acl-number* }]

no ip pim rp-candidate [*interface-type interface-number*]

default ip pim rp-candidate [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Name of an interface whose IP address is used as the C-RP address.

priority-value: RP priority. The value range is from 0 to 255, and the default value is **192**.

interval: Interval of sending C-RP messages to the BSR. The value range is from 1 to 16383, and the default value is **60** seconds.

group-list *acl-name*: Uses a standard IP ACL name to limit the address range of groups served by this C-RP. The value is a case-sensitive string of 1 to 99 characters. By default, a C-RP serves all groups.

group-list *acl-number*: Uses a standard IP ACL number to limit the address range of groups served by this C-RP. The value range is from 1 to 99. By default, the C-RP serves all groups.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In PIM-SM, a rendezvous point tree (RPT) created based on multicast routing data takes the RP as a root and group members as leaves. An RP is elected from C-RPs. After a BSR is elected, all C-RPs periodically send unicast messages to the BSR and then the BSR forwards the messages throughout the PIM domain.

When an ACL is used to specify the address range of groups served by the C-RP, only the permit access control entry (ACE) is calculated, and the deny ACE is not calculated.

Examples

The following example sets the address of GigabitEthernet 0/1 to the C-RP address, the RP priority to 200, and the interval of sending C-RP messages to the BSR to 70 seconds, and uses the ACL to limit the address range of groups served by the C-RP to 225.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 3 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim rp-candidate GigabitEthernet 0/1 priority 200 group-list
3 interval 70
```

Notifications

If the multicast function is not enabled on an interface, the following notification will be displayed:

```
Warning: PIMSM not configured on %s, Candidate-RP not advertised
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 ip pim rp-register-kat

Function

Run the **ip pim rp-register-kat** command to configure the (S, G) entry timeout period on the RP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the (S, G) entry timeout period is the sum of three times the register suppression time and the register-probe time.

Syntax

ip pim rp-register-kat *interval*

no ip pim rp-register-kat
default ip pim rp-register-kat

Parameter Description

Interval: (S, G) entry timeout period on the RP, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the (S, G) entry timeout period to 250 seconds on the RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim rp-register-kat 250
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ip pim sparse-mode

Function

Run the **ip pim sparse-mode** command to enable the PIM-SM function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.
The PIM-SM function is disabled on an interface by default.

Syntax

ip pim sparse-mode

no ip pim sparse-mode

default ip pim sparse-mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before PIM-SM is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-SM is enabled.

It is not recommended that different IPv4 multicast routing protocols be configured on interfaces of a device.

When PIM-SM is enabled, IGMP is automatically enabled on different interfaces.

The multicast function can be enabled on a tunnel interface that does not support multicast. In this case, no notification will be displayed and multicast packets will not be sent or received.

A multicast tunnel cannot be nested and does not support multicast data QoS/ACL.

Examples

The following example enables the PIM-SM function on GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
```

Notifications

If the specified interface does not exist, the following notification will be displayed:

```
ip pim sparse-mode (vif == NULL)
```

If the multicast function is not enabled, the following notification will be displayed:

```
WARNING:  \"ip multicast-routing\"  is not configured, PIM Sparse-mode
```

If the interfaces exceed the upper limit, the following notification will be displayed:

```
PIM-SM Configure failed! VIF limit exceeded in NSM!!!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

1.29 ip pim sparse-mode passive

Function

Run the **ip pim sparse-mode passive** command to enable the PIM-SM passive mode on an interface.

Run the **no** form of this command to disable this mode.

Run the **default** form of this command to restore the default configuration.

The PIM-SM passive mode is disabled on an interface by default.

Syntax

ip pim sparse-mode passive

no ip pim sparse-mode passive

default ip pim sparse-mode passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before the PIM-SM passive mode is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if the PIM-SM passive mode is enabled.

When the PIM-SM passive mode is enabled, IGMP is automatically enabled on different interfaces.

After the PIM-SM passive mode is enabled on an interface, the interface does not receive or send PIM packets, but it can forward multicast packets. It is recommended that the PIM-SM passive mode be enabled on an interface of a stub network device connected to hosts. This avoids L2 flooding of the PIM hello messages.

Examples

The following example enables the PIM-SM passive mode on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim sparse-mode passive
```

Notifications

N/A

Common Errors

The PIM-SM passive mode is enabled on an interface connected to a source. The source interface does not send or receive PIM packets; therefore, it loses the DR election capability. It is not recommended that the PIM-SM passive mode be enabled on an interface connected to a source.

After the PIM-SM passive mode is enabled on an interface, if two devices in the same network segment forward multicast data, assertion election cannot proceed. As a result, two identical multicast packets are sent to this network segment.

If the PIM-SM passive mode is enabled on an interface of an intermediate device deployed on an L3 multicast network, the networking fails because the interface does not receive or send PIM packets.

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

1.30 ip pim sparse-mode subvlan

Function

Run the **ip pim sparse-mode subvlan** command to enable the PIM-SM function for sub VLANs of a super VLAN interface.

Run the **no** form of this command to disable this function for sub VLANs of a super VLAN interface.

Run the **default** form of this command to restore the default configuration.

The PIM-SM function is disabled on a super VLAN interface by default.

Syntax

ip pim sparse-mode subvlan { **all** | *vlan-id* }

no ip pim sparse-mode subvlan

default ip pim sparse-mode subvlan

Parameter Description

all: Sends PIM-SM protocol packets to all sub VLANs.

vlan-id: ID of a sub VLAN to which PIM-SM protocol packets are sent.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Generally, a super VLAN contains many sub VLANs. If PIM-SM is enabled on a super VLAN interface, the super VLAN interface duplicates the protocol packets and sends them to all sub VLANs. If the number of sub VLANs is too many, exceeding the processing capability of the device, packets are discarded, resulting in protocol flapping.

In most scenarios, the PIM-SM protocol is disabled by default and not needed on a super VLAN interface. This interface does not send or receive PIM packets. If the PIM-SM protocol is needed on a super VLAN interface in some scenarios, you can run this command to enable the protocol.

Examples

The following example enables PIM-SM packets to be sent to sub VLAN 200 on super VLAN 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 100
Hostname(config-vlan)# supervlan
Hostname(config-vlan)# interface vlan 100
Hostname(config-if-vlan 100)# ip pim sparse-mode subvlan 200
```

Notifications

If this command is run on a non-super VLAN interface, the following notification will be displayed:

```
%% this command can apply to supervlan switch virtual interface only.
```

If the specified sub VLAN ID is consistent with the VLAN ID of an SVI, the following notification will be displayed:

```
%% subvlan vid(%d) is equal to SVI vlan id, not support
```

Common Errors

- This command is run on a non-super VLAN interface.
- The sub VLAN specified on a super VLAN interface cannot communicate with neighbors.

Platform Description

N/A

Related Commands

N/A

1.31 ip pim spt-threshold

Function

Run the **ip pim spt-threshold** command to enable the shortest path tree (SPT) switchover function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SPT switchover function is disabled by default.

Syntax

ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

no ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

default ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

Parameter Description

group-list *acl-name*: Uses a standard IP ACL name to limit the address range of groups that support SPT switchover. The value is a case-sensitive string of 1 to 99 characters.

group-list *acl-number*: Uses a standard IP ACL number to limit the address range of groups that support SPT switchover. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** parameter is not specified, all groups support SPT switchover.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits on the ACL associated with the **group-list** parameter are removed. In this case, all groups are allowed to switch over from an RPT to an SPT.

Examples

The following example uses ACL 12 to specify the multicast group with the address 225.1.1.1 and reverse mask 0.0.0.255 to support SPT switchover.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 12 permit 225.1.1.1 0.0.0.255
```

```
Hostname(config)# ip pim spt-threshold group-list 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 ip pim ssm

Function

Run the **ip pim ssm** command to enable the SSM function and configure an SSM group address range.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SSM function is disabled by default.

Syntax

ip pim ssm { **default** | **range** { *acl-name* | *acl-number* } }

no ip pim ssm

default ip pim ssm

Parameter Description

default: Specifies the default SSM group address range. The value range is from 232.0.0.0 to 232.0.0.8.

range *acl-name*: Uses a standard IP ACL name to limit the SSM group address range. The value is a case-sensitive string of 1 to 99 characters.

range *acl-number*: Uses a standard IP ACL number to limit the SSM group address range. The value range is from 1 to 99.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If SSM applications must be implemented in the PIM-SM network, this command must be run.

Examples

The following example enables the SSM function and sets the SSM group address range to 232/8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim ssm default
```

The following example enables the SSM function and sets the SSM group address range to 226/8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 10 permit 226.0.0.1 0.0.0.255
Hostname(config)# ip pim ssm range 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp ssm-map enable** (IGMP)
- **ip igmp ssm-map static** (IGMP)
- **show ip igmp ssm-mapping** (IGMP)

1.33 ip pim triggered-hello-delay

Function

Run the **ip pim triggered-hello-delay** command to configure the hello message sending delay on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.
The default hello message sending delay is **5** seconds.

Syntax

ip pim triggered-hello-delay *delay*
no ip pim triggered-hello-delay
default ip pim triggered-hello-delay

Parameter Description

delay: Hello message sending delay, in seconds. The value range is from 1 to 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When a PIM interface is enabled or detects a new neighbor, a random time is generated. Within the time, the interface sends hello messages.

Examples

The following example sets the hello message sending delay to 3 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim triggered-hello-delay 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.34 show ip pim sparse-mode bsr-router

Function

Run the **show ip pim sparse-mode bsr-router** command to display BSR information.

Syntax

show ip pim sparse-mode bsr-router

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SM BSR information.

```
Hostname> enable
```

```
Hostname# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.127.1
Uptime:  01d23h14m, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:42
Role: Candidate BSR   Priority: 64, Hash mask length: 10
State: Elected BSR
Candidate RP: 30.30.100.200(GigabitEthernet 0/3)
Advertisement interval 60 seconds
00:00:32
```

Table 1-1 Output Fields of the show ip pim sparse-mode bsr-router Command

Field	Description
BSR address	BSR address
Uptime	Update time
BSR Priority	BSR priority
Hash mask length	Hash mask length
Next bootstrap message in *time*	Next bootstrap time
Role	BSR role
Priority	Priority
Hash mask length	Hash mask length
State	BSR status
Candidate RP	C-RP address
Advertisement interval *interval* seconds	C-RP advertisement interval
Next Cand_RP_advertisement in *time*	Next C-RP advertisement time

Notifications

N/A

Platform Description

N/A

1.35 show ip pim sparse-mode interface

Function

Run the **show ip pim sparse-mode interface** command to display PIM-SM information of an interface.

Syntax

show ip pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

interface-type interface-number: Specified interface. If this parameter is not specified in the command, information of all interfaces is displayed.

detail: Displays details of interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SM information of an interface.

```
Hostname> enable
Hostname# show ip pim sparse-mode interface detail
GigabitEthernet 0/3 (vif 3):
  Address 30.30.100.200, DR 30.30.100.200
  Hello period 30 seconds, Next Hello in 11 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   2.2.2.2
```

Table 1-2 Output Fields of the show ip pim sparse-mode interface detail Command

Field	Description
Address	Interface address
DR	Address of a DR in the same shared network segment as the interface
Hello period *hello-interval* seconds	Hello message sending interval: *hello-interval* seconds
Next Hello in *next-hello-time* seconds	Next hello message *next-hello-time* seconds later
Triggered Hello period *triggered-hello-time* seconds	Triggered-Hello-Delay of an interface: *triggered-hello-time* seconds
Neighbors	Neighbors on an interface

Notifications

N/A

Platform Description

N/A

1.36 show ip pim sparse-mode local-members

Function

Run the **show ip pim sparse-mode local-members** command to display local IGMP information of a PIM-SM interface.

Syntax

show ip pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays local IGMP information of a PIM-SM interface.

```
Hostname> enable
Hostname# show ip pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/3:
(*, 225.1.1.1) : Include
```

Table 1-3 Output Fields of the show ip pim sparse-mode local-members Command

Field	Description
PIM Local membership information	Local member information
interface-type interface-number	Interface name
(*source*, *ip-group-address*): mode	(S, G): source filtering mode

Notifications

N/A

Platform Description

N/A

1.37 show ip pim sparse-mode mroute

Function

Run the **show ip pim sparse-mode mroute** command to display PIM-SM routing information.

Syntax

show ip pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter Description

***group-or-source-address*: Group address or source address. The two addresses must be one group address and one source address. Command Modes**

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Either a source address or a group address can be specified.

A source address and a group address can be specified together.

The two addresses must be one group address and one source address.

Examples

The following example displays the PIM-SM routing information.

```
Hostname> enable
Hostname# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(192.168.1.100, 233.3.3.3)
RPF nbr: 192.168.36.90
RPF idx: VLAN 1
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 49 seconds
```

```
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
```

Table 1-4 Output Fields of the show ip pim sparse-mode mroute Command

Field	Description
IP Multicast Routing Table	IP multicast routing table
(*,*,RP) Entries	Number of (*, *, RP) entries
(*,G) Entries	Number of (*, G) entries
(S,G) Entries	Number of (S, G) entries
(S,G,rpt) Entries	Number of (S, G, RPT) entries
FCR Entries	Number of FCR entries
REG Entries	Number of register entries

Field	Description
RPF nbr	RPF neighbor
RPF idx	RPF interface index
SPT bit	SPT flag bit: 0 or 1 ● **0**: No multicast data is received. ● **1**: Multicast data is received.
Upstream State	Uplink neighbor status includes PRUNED, NOT PRUNED, JOINED, NOT JOINED, PRUNE_PENDING, and RPT NOT JOINED.
jt_timer expires in *jt-expire-time* seconds	Prune expires *jt-expire-time* seconds later.
kat expires in *kat-expire-time* seconds	(S, G) entry expires *kat-expire-time* seconds later.
Local	Inbound interface of a local multicast group
Pruned	Inbound interface for receiving prune packets
Joined	Inbound interface for receiving join packets
Asserted	Inbound interface for receiving assert packets
Outgoing	Outbound interface for forwarding entries

Notifications

N/A

Platform Description

N/A

1.38 show ip pim sparse-mode neighbor

Function

Run the **show ip pim sparse-mode neighbor** command to display neighbor information.

Syntax

show ip pim sparse-mode neighbor [**detail**]

Parameter Description

detail: Displays details. If this parameter is not specified, the summary information of neighbors is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SM neighbor information.

```
Hostname> enable
Hostname# show ip pim sparse-mode neighbor
Neighbor         Interface                 Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
10.0.0.2         GigabitEthernet 0/23        02:01:23/00:01:21   v2    1 / DR
```

Table 1-5 Output Fields of the show ip pim sparse-mode neighbor Command

Field	Description
Neighbor	Neighbor
Interface	Interface
Uptime/Expires	Update time/expiry time
Ver	Version
DR Address	DR address
Priority/Mode	Priority/Mode

Notifications

N/A

Platform Description

N/A

1.39 show ip pim sparse-mode nexthop

Function

Run the **show ip pim sparse-mode nexthop** command to display next hop information, including interface number, address, and metric value of a next hop.

Syntax

show ip pim sparse-mode nexthop

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the PIM-SM next hop information.

```
Hostname> enable
Hostname# show ip pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination    Type  Nexthop   Nexthop        Nexthop              Metric Pref
Refcnt
                     Num     Addr           Name
_____________________________________________________________________________
__________
20.0.0.1       R  1        0.0.0.0        GigabitEthernet 0/24     0      0     2
30.0.0.2       S  1        20.0.0.1       GigabitEthernet 0/24     2      110   2
```

Table 1-6 Output Fields of the show ip pim sparse-mode nexthop Command

Field	Description
Destination	Destination address
Type	Type
Nexthop Num	Number of next hops
Nexthop Addr	Next hop address
Nexthop Name	Outbound interface of next hop
Metric	Number of hops to reach the destination address
Pref	Priority of unicast route to reach the destination address
Refcnt	Reference count

Notifications

N/A

Platform Description

N/A

1.40 show ip pim sparse-mode rp-hash

Function

Run the **show ip pim sparse-mode rp-hash** command to display RP information corresponding to a multicast group address.

Syntax

show ip pim sparse-mode rp-hash *group-address*

Parameter Description

group-address: Address of a multicast group resolved.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RP information corresponding to a group address 225.1.1.1.

```
Hostname> enable
Hostname# show ip pim sparse-mode rp-hash 225.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

Table 1-7 Output Fields of the show ip pim sparse-mode rp-hash Command

Field	Description
RP	RP address
Info source	Address of a source that sends information
via bootstrap	Messages from a BSR

Notifications

N/A

Platform Description

N/A

1.41 show ip pim sparse-mode rp mapping

Function

Run the **show ip pim sparse-mode rp mapping** command to display all RPs and the groups served by the RPs on the local device.

Syntax

show ip pim sparse-mode rp mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all RPs and the groups served by the RPs on the local device.

```
Hostname> enable
Hostname# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 30.30.200.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:00:51, expires: 00:01:39
RP: 30.30.100.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:19:14, expires: 00:01:38
Group(s): 224.0.0.0/4, Static
RP: 100.100.100.100
Uptime: 00:45:35
```

Table 1-8 Output Fields of the show ip pim sparse-mode rp mapping Command

Field	Description
Group(s)	Address/Mask of a group
RP	RP address
Info source	Address of a source that sends information
via bootstrap	Messages from a BSR

Field	Description
priority	Priority
Uptime	Update time
expires	Expiry time

Notifications

N/A

Platform Description

N/A

1.42 show ip pim sparse-mode track

Function

Run the **show ip pim sparse-mode track** command to display the number of PIM packets sent and received since the statistic start time.

Syntax

show ip pim sparse-mode track

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the system is started for the first time, the statistic start time is set. If you run the **clear ip pim sparse-mode track** command, the statistic start time and the PIM packet counter are reset.

Examples

The following example displays the number of PIM packets sent and received since the statistic start time.

```
Hostname> enable
Hostname# show ip pim sparse-mode track
             PIM packet counters track
Elapsed time since counters cleared: 00:04:03
                    received   sent
Valid PIMSM packets:    0         8
Hello:                 0         8
```

```
Join-Prune:           0          0
Register:             0          0
Register-Stop:         0          0
Assert:               0          0
BSM:                  0          0
C-RP-ADV:             0          0
PIMDM-Graft:          0
PIMDM-Graft-Ack :      0
PIMDM-State-Refresh:    0
Unknown PIM Type:      0
Errors:
Malformed packets:     0
Bad checksums:         0
Send errors:           0
Packets received with unknown PIM version:  0
```

Figure 1-1 Output Fields of the show ip pim sparse-mode track Command

Field	Description
Elapsed time since counters cleared	Duration since the statistic start time till now
Received	Number of received PIM packets
sent	Number of sent PIM packets
Valid PIMSM packets	Valid PIM-SM packets
Hello	Statistical value of hello messages
Join-Prune	Statistical value of join-prune packets
Register	Statistical value of register messages
Register-Stop	Statistical value of register-stop packets
Assert	Statistical value of assert packets
BSM	Statistical value of BSMs
C-RP-ADV	Statistical value of C-RP advertisement packets
PIMDM-Graft	Statistical value of PIM-DM graft packets
PIMDM-Graft-Ack	Statistical value of PIM-DM graft acknowledgment packets
PIMDM-State-Refresh	Statistical value of PIM-DM SRMs
Unknown PIM Type	Unknown PIM packets
Errors	Statistical value of error packets
Malformed packets	Number of malformed packets

Field	Description
Bad checksums	Number of packets with incorrect checksums
Send errors	Number of sent error packets
Packets received with unknown PIM version	Number of PIM packets with unknown version

Notifications

N/A

Platform Description

N/A

1 PIM-DM Commands

Command	Function
clear ip pim dense-mode track	Clear statistical information about PIM-DM packets.
ip pim bfd	Enable the PIM-BFD function on an interface.
ip pim dense-mode	Enable the PIM-DM function on an interface.
ip pim dense-mode passive	Enable the PIM-DM passive mode on an interface.
ip pim dense-mode subvlan	Enable the PIM-DM function on a super VLAN interface.
ip pim neighbor-filter	Enable the neighbor filtering function on an interface.
ip pim override-interval	Configure the prune override interval of hello messages.
ip pim propagation-delay	Configure the propagation delay of hello messages.
ip pim query-interval	Configure the hello message sending interval.
ip pim state-refresh disable	Disable the PIM-DM state refresh function on an interface.
ip pim state-refresh origination-interval	Configure the PIM-DM SRM sending interval on an interface.
ip pim mib dense-mode	Switch over the management object of the MIB function from PIM-SM to PIM-DM.
show ip pim dense-mode interface	Display information of a PIM-DM interface.
show ip pim dense-mode mroute	Display PIM-DM routing entry information.
show ip pim dense-mode neighbor	Display PIM-DM neighbor information.
show ip pim dense-mode nexthop	Display PIM-DM next hop information.
show ip pim dense-mode track	Display statistical information about PIM-DM packets.

1.1 clear ip pim dense-mode track

Function

Run the **clear ip pim dense-mode track** command to clear statistical information about PIM-DM packets.

Syntax

clear ip pim dense-mode track

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command resets the statistic start time and clears the counter of PIM-DM packets.

Examples

The following example clears statistical information about the PIM-DM packets.

```
Hostname> enable
Hostname# clear ip pim dense-mode track
```

Notifications

N/A

Platform Description

N/A

1.2 ip pim bfd

Function

Run the **ip pim bfd** command to enable the PIM-BFD function on an interface.

Run the **no** form of this command to disable this function.

The PIM-BFD function is disabled on an interface by default.

Syntax

ip pim bfd

no ip pim bfd

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Bidirectional forwarding detection (BFD) is a detection mechanism applying to an entire network and it is used to quickly detect or monitor links or IP route forwarding connectivity in a network.

PIM-DM uses the assertion election mechanism. The assertion winning device functions as a unique forwarder of multicast data in a shared network. If multiple devices in a shared network receive multicast data concurrently, they forward the data to the same devices. These devices mutually transmit assert packets and elect a winning device based on the assert packets. The winning device forwards traffic. When the neighbor interface changes, the change can be quickly detected by BFD correlation and a new round of election can be initiated.

Examples

The following example enables the PIM-BFD function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim dense-mode**
- **show bfd neighbors** (reliability/BFD)

1.3 ip pim dense-mode

Function

Run the **ip pim dense-mode** command to enable the PIM-DM function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.

The PIM-DM function is disabled on an interface by default.

Syntax

ip pim dense-mode

no ip pim dense-mode

default ip pim dense-mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The PIM-DM function must be enabled on an interface to process PIM packets of PIM neighbors so that a PIM-DM network can be constructed. PIM-DM can effectively solve multicast data transmission of small networks with densely located hosts. You are advised to enable PIM-DM on all L3 interfaces of the PIM-DM network and configure the same IPv4 multicast routing protocol on interfaces of a device.

Before PIM-DM is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, the PIM-DM function does not take effect. When PIM-DM is enabled, IGMP is automatically started on different interfaces.

For tunnel interfaces, only 4Over4, 4Over4 GRE, 4Over6, and 4Over6 GRE support the IPv4 multicast function. The multicast function can be enabled on a tunnel interface that does not support multicast. In this case, no notification is displayed and multicast packets are not sent or received through this interface. A multicast tunnel must be created on an Ethernet interface, and it cannot be nested and does not support multicast data QoS/ACL.

Examples

The following example enables the PIM-DM function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim dense-mode
```

Notifications

If the multicast routing function is not enabled on a device, the following notification will be displayed:

```
WARNING:  "ip multicast-routing"  is not configured, PIM Dense-mode will not
start-up.
```

If the number of multicast interfaces on a device reaches the upper limit, the following notification will be displayed:

```
Operation failed: PIM-DM VIF limit exceeded
```

If the interface is not added to the global VRF, the following notification will be displayed:

```
PIM-DM allow to configure on vrf 0 only
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

1.4 ip pim dense-mode passive

Function

Run the **ip pim dense-mode passive** command to enable the PIM-DM passive mode on an interface.

Run the **no** form of this command to disable this mode on an interface.

Run the **default** form of this passive command to restore the default configuration.

The PIM-DM passive mode is disabled on an interface by default.

Syntax

ip pim dense-mode passive

no ip pim dense-mode passive

default ip pim dense-mode passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before the PIM-DM passive mode is enabled, enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-DM passive mode is enabled.

When the PIM-DM passive mode is enabled, IGMP is automatically enabled on different interfaces.

After the PIM-DM passive mode is enabled on an interface, the interface does not receive or send PIM packets, but it can forward multicast packets. You are advised to enable the PIM-DM passive mode on an interface of a stub network device connected to hosts. This avoids L2 flooding of the PIM hello messages.

Examples

The following example enables the PIM-DM passive mode on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip pim dense-mode passive
```

Notifications

If the multicast routing function is not enabled on a device, the following notification will be displayed:

```
WARNING: "ip multicast-routing" is not configured, PIM Dense-mode passive will
not start-up.
```

If the number of multicast interfaces on a device reaches the upper limit, the following notification will be displayed:

```
Operation failed: PIM-DM VIF limit exceeded
```

If the interface is not added to the global VRF, the following notification will be displayed:

```
PIM-DM allow to configure on vrf 0 only
```

Common Errors

If two devices in a network segment forward multicast packets, assertion election cannot proceed. If the **pim dense-mode passive** mode is enabled on the interface, the assertion election mechanism fails. As a result, two identical multicast packets are sent to this network segment.

If the **pim dense-mode passive** mode is enabled on an interface of an intermediate device deployed on an L3 multicast network, the networking fails because the interface does not receive or send PIM packets.

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

1.5 ip pim dense-mode subvlan

Function

Run the **ip pim dense-mode subvlan** command to enable the PIM-DM function on a super VLAN interface.

Run the **no** form of this command to disable this function on a super VLAN interface.

Run the **default** form of this command to restore the default configuration.

The PIM-DM function is disabled on a super VLAN interface by default.

Syntax

ip pim dense-mode subvlan [**all** | *subvlan-id*]

no ip pim dense-mode subvlan

default ip pim dense-mode subvlan

Parameter Description

all: Specifies that PIM-DM packets are sent to all sub VLANs.

subvlan-id: ID of a sub VLAN to which PIM-DM packets are sent. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Generally, a super VLAN contains many sub VLANs. If PIM-DM is enabled on a super VLAN interface, the super VLAN interface duplicates the protocol packets and sends them to all sub VLANs. If the number of sub VLANs is too many, exceeding the processing capability of the device, packets are discarded, resulting in protocol flapping.

In most scenarios, the PIM-DM protocol is disabled by default and not needed on a super VLAN interface. This interface does not send or receive PIM packets. If the PIM-DM protocol is needed on a super VLAN interface in some scenarios, you can run this command to enable the protocol. Note that if all sub VLANs are specified to receive packets, the transmission performance may be reduced, causing neighbor flapping.

Examples

The following example enables the PIM-DM function on the super VLAN interface with VLAN 100 and specifies PIM packets to be sent to sub VLAN 200.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 100
Hostname(config-if-vlan 100)# ip pim dense-mode subvlan 200
```

Notifications

If this command is run on a non-super VLAN interface, the following notification will be displayed:

```
%% this command can apply to supervlan switch virtual interface only.
```

If the specified sub VLAN ID is consistent with the VLAN ID of an SVI, the following notification will be displayed:

```
%% subvlan vid(%d) is equal to SVI vlan id, not support
```

Common Errors

- This command is run on a non-super VLAN interface.
- The sub VLAN specified on a super VLAN interface cannot communicate with neighbors.

Platform Description

N/A

Related Commands

N/A

1.6 ip pim neighbor-filter

Function

Run the **ip pim neighbor-filter** command to enable the neighbor filtering function on an interface.

Run the **no** form of this command to disable this function on the interface.

Run the **default** form of this command to restore the default configuration.

The neighbor filtering function is disabled on an interface by default.

Syntax

ip pim neighbor-filter { *acl-name* | *acl-number* }

no ip pim neighbor-filter { *acl-name* | *acl-number* }

default ip pim neighbor-filter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a standard IP ACL. The value is a case-sensitive string of 1 to 99 characters.

acl- number: No. of a standard IP ACL. The value range is from 1 to 99.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a neighbor is filtered out based on an access filtering list, PIM-DM does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

Only addresses that meet ACL filtering conditions can be used as PIM neighbors of the current interface. Otherwise, the addresses filtered out cannot be neighbors. Peering refers to exchange of protocol packets between PIM neighbors. If peering with a PIM device is suspended, the neighbor relationship with it cannot be formed so that PIM protocol packets will not be received from the device.

Examples

The following example enables the neighbor filtering function on GigabitEthernet 0/1 and uses ACL 14 as the filtering rule.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim neighbor-filter 14
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

[™]

- **show ip pim dense-mode interface**

1.7 ip pim override-interval

Function

Run the **ip pim override-interval** command to configure the prune override interval of hello messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default prune override interval of hello messages is **2500** ms.

Syntax

ip pim override-interval *override-interval*

no ip pim override-interval

default ip pim override-interval

Parameter Description

override-interval: Prune override interval of hello messages, in milliseconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the prune override interval of hello messages to 3000 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim override-interval 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip pim propagation-delay
- show ip pim dense-mode interface

1.8 ip pim propagation-delay

Function

Run the **ip pim propagation-delay** command to configure the propagation delay of hello messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default propagation delay of hello messages on an interface is **500** ms.

Syntax

ip pim propagation-delay *propagation-delay-time*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description

propagation-delay-time: Propagation delay of hello messages, in milliseconds. The value range is from 1 to 32767.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the propagation delay of hello messages to 600 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim propagation-delay 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip pim override-interval**
- **show ip pim dense-mode interface**

1.9 ip pim query-interval

Function

Run the **ip pim query-interval** command to configure the hello message sending interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Hello messages are sent at an interval of **30** seconds by default.

Syntax

ip pim query-interval *query-interval*

no ip pim query-interval

default ip pim query-interval

Parameter Description

query-interval: Hello message sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the hello message sending interval is configured, the hello message hold time is updated as a product of 3.5 and the hello message sending interval.

Examples

The following example sets the hello message sending interval to 123 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim query-interval 123
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim dense-mode interface**

1.10 ip pim state-refresh disable

Function

Run the **ip pim state-refresh disable** command to disable the PIM-DM state refresh function on an interface.

Run the **no** form of this command to restore the PIM-DM state refresh function on an interface.

Run the **default** form of this command to restore the default configuration.

The PIM-DM SRMs are processed and forwarded by default.

Syntax

ip pim state-refresh disable

no ip pim state-refresh disable

default ip pim state-refresh disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the PIM state refresh function is disabled, SRMs are not processed or forwarded. The SR Cap option is not included in a hello message, and is not processed when the hello message is received.

Disabling the PIM-DM state refresh function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, you are not advised to disable this function in general conditions.

Examples

The following example disables the PIM-DM state refresh function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config-if-GigabitEthernet 0/1)# ip pim state-refresh disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ip pim state-refresh origination-interval

Function

Run the **ip pim state-refresh origination-interval** command to configure the PIM-DM SRM sending interval on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The PIM-DM SRMs are sent at an interval of **60** seconds by default.

Syntax

ip pim state-refresh origination-interval *origination-interval*

no ip pim state-refresh origination-interval

default ip pim state-refresh origination-interval

Parameter Description

origination-interval: PIM-DM SRM sending interval, in seconds. The value range is from 1 to 100.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the PIM-DM SRM sending interval to 65 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip pim state-refresh origination-
interval 65
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip pim mib dense-mode

Function

Run the **ip pim mib dense-mode** command to switch over the management object of the MIB function from PIM-SM to PIM-DM.

Run the **no** form of this command to switch over the management object of the MIB function from PIM-DM to PIM-SM.

Run the **default** form of this command to restore the default configuration.

PIM-SM is managed by the MIB function by default.

Syntax

ip pim mib dense-mode
no ip pim mib dense-mode

default ip pim mib dense-mode

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example switches over the management object of the MIB function from PIM-SM to PIM-DM.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip pim mib dense-mode
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show ip pim dense-mode interface

Function

Run the **show ip pim dense-mode interface** command to display information of a PIM-DM interface.

Syntax

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

interface-type interface-number: Specified interface type and interface number, used to display information of this PIM-DM interface.

detail: Displays detailed information of an interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of a PIM-DM interface.

```
Hostname> enable
Hostname# show ip pim dense-mode interface
Address      Interface          VIF     Ver/    Nbr
                              Index    Mode    Count
10.10.10.10   FastEthernet 0/45   3       v2/D    1
50.50.50.50   VLAN 4              2       v2/D    1
```

Table 1-1 Output Fields of the show ip pim dense-mode interface Command

Field	Description
Address	Primary IP address of a PIM-DM interface
Interface	Name of a PIM-DM interface
VIF Index	VIF ID
Ver/Mode	PIM version and mode
Nbr Count	Number of neighbors on a PIM-DM interface

Notifications

N/A

Platform Description

N/A

1.14 show ip pim dense-mode mroute

Function

Run the **show ip pim dense-mode mroute** command to display PIM-DM routing entry information.

Syntax

show ip pim dense-mode mroute [*group-or-source-address-1* [*group-or-source-address-2*]] [**summary**]

Parameter Description

group-or-source-address-1: Group address or source address.

group-or-source-address-2: Group address or source address. The two addresses must be one group address and one source address.

summary: Displays summary of routing entries.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-DM routing entry information.

```
Hostname> enable
Hostname# show ip pim dense-mode mroute
```

```
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
MRT lifetime expires in 205 seconds
RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4
Upstream IF: VLAN 4
Upstream State: Pruned, PLT:200
Assert State: NoInfo
Downstream IF List:
FastEthernet 0/45:
Downstream State: NoInfo
Assert State: Loser, AT:170
```

Table 1-2 Output Fields of the show ip pim dense-mode mroute Command

Field	Description
RPF Neighbor	RPF neighbor
Nexthop	IP address and interface of the RPF next hop
Upstream IF	Interface connected to an upstream neighbor
Upstream State	State of an upstream neighbor
Assert State	Assert state of an upstream interface
Downstream IF List	List of interfaces connected to downstream neighbors
Downstream State	State of a downstream neighbor
Assert State	Assert state of a downstream interface

Notifications

N/A

Platform Description

N/A

1.15 show ip pim dense-mode neighbor

Function

Run the **show ip pim dense-mode neighbor** command to display PIM-DM neighbor information.

Syntax

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Specified interface type and interface number, used to display PIM-DM neighbor information of this interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the PIM-DM neighbor information.

```
Hostname> enable
Hostname# show ip pim dense-mode neighbor
Neighbor-Address   Interface         Uptime/Expires     Ver
10.10.10.1        FastEthernet 0/45   00:19:29/00:01:21   v2
50.50.50.1        VLAN 4            00:22:09/00:01:39   v2
```

Table 1-3 Output Fields of the show ip pim dense-mode neighbor Command

Field	Description
Neighbor-Address	Neighbor address
Interface	Interface connected to neighbors
Uptime/Expires	Entry timeout period/aging time
Ver	PIM version

Notifications

N/A

Platform Description

N/A

1.16 show ip pim dense-mode nexthop

Function

Run the **show ip pim dense-mode nexthop** command to display PIM-DM next hop information.

Syntax

show ip pim dense-mode nexthop

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the PIM-DM next hop information.

```
Hostname> enable
Hostname# show ip pim dense-mode nexthop
Destination   Nexthop   Nexthop     Nexthop    Metric   Pref
            Num      Addr        Interface
1.1.1.111    1        50.50.50.1   VLAN 4     0       1
```

Table 1-4 Output Fields of the show ip pim dense-mode nexthop Command

Field	Description
Destination	Address of a multicast source
Nexthop Num	Number of next hops
Nexthop Addr	Next hop address
Nexthop Interface	Interface connected to a next hop
Metric	Metric of a route
Pref	Route priority

Notifications

N/A

Platform Description

N/A

1.17 show ip pim dense-mode track

Function

Run the **show ip pim dense-mode track** command to display statistical information about PIM-DM packets.

Syntax

show ip pim dense-mode track

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the system is started, the statistic start time is set. Each time the **ip pim dense-mode track** command is run, the statistic start time is reset and the PIM packet counter is cleared.

Examples

The following example displays statistical information about PIM-DM packets.

```
Hostname> enable
Hostname# show ip pim dense-mode track
               PIM packet counters
Elapsed time since counters cleared: 00:04:03
              Received   sent
Valid PIMDM packets:  1         8
Hello:              1         8
Join/Prune:          0         0
Graft:              0         0
Graft-Ack:           0         0
Assert:             0         0
State-Refresh:       0         0
PIM-SM-Register:     0         0
PIM-SM-Register-Stop: 0         0
PIM-SM-BSM:          0         0
PIM-SM-RP-ADV:     0         0
Unknown Type:        0
Errors:
Malformed packets:    0
Bad checksums:       0
Unknown PIM version:  0
Send errors:         0
```

Table 1-5 Output Fields of the show ip pim dense-mode nexthop Command

Field	Description
Elapsed time since counters cleared	Duration since the statistic start time till now

Field	Description
Received	Number of received PIM packets
sent	Number of sent PIM packets
Valid PIMDM packets	Valid PIM-DM packets
Hello	Statistical value of hello messages
Join/Prune	Statistical value of join-prune packets
Graft	Statistical value of graft packets
Graft-Ack	Statistical value of graft acknowledgment packets
Assert	Statistical value of assert packets
State-Refresh	Statistical value of SRMs
PIM-SM-Register	Statistical value of register messages
PIM-SM-Register-Stop	Statistical value of register-stop packets
PIM-SM-BSM	Statistical value of BSMs
PIM-SM-RP-ADV	Statistical value of C-RP advertisement packets
Unknown Type	Unknown PIM packets
Errors	Error packets
Malformed packets	Number of malformed packets
Bad checksums	Number of packets with incorrect checksums
Unknown PIM version	Number of PIM packets with unknown version
Send errors	Number of sent error packets

Notifications

N/A

Platform Description

N/A

1 IGMP Snooping Commands

Command	Function
clear ip igmp snooping gda-table	Clear dynamic forwarding entries.
clear ip igmp snooping statistics	Clear IGMP snooping statistics.
deny	Deny a range of multicast groups specified by a profile.
ip igmp profile	Create a profile and enter the profile configuration mode.
ip igmp snooping dyn-mr-aging-time	Configure the aging time of dynamic multicast router ports.
ip igmp snooping fast-leave enable	Enable the port fast leave function.
ip igmp snooping filter	Apply a profile to a port to restrict the multicast groups that user hosts connecting to the port can join.
ip igmp snooping vlan filter	Apply a profile to a VLAN to restrict the multicast groups that user hosts in the VLAN can join.
ip igmp snooping host-aging-time	Configure the aging time for IGMP snooping dynamic member ports.
ip igmp snooping ivgl	Enable IGMP snooping globally and run the Independent VLAN Group Learning (IVGL) mode.
ip igmp snooping ivgl-svgl	Enable IGMP snooping globally and run the IVGL-SVGL mode.
ip igmp snooping l2-entry-limit	Configure the maximum number of multicast groups allowed for concurrent request globally.
ip igmp snooping limit-ipmc vlan address server	Specify a multicast group address and multicast source address for a VLAN.
ip igmp snooping max-groups	Configure the maximum number of multicast groups that can be dynamically learned by a port.
ip igmp snooping mrouter learn pim-dvmrp	Enable the function of dynamic multicast router port learning.
ip igmp snooping preview	Enable the multicast preview function.
ip igmp snooping preview interval	Configure the multicast preview duration.

ip igmp snooping querier	Enable the IGMP snooping querier function.
ip igmp snooping querier address	Configure the source IP address of the IGMP snooping querier.
ip igmp snooping querier max-response-time	Configure the maximum response time of IGMP snooping queriers.
ip igmp snooping querier query-interval	Configure the interval for an IGMP snooping querier to send Query packets.
ip igmp snooping querier timer expiry	Configure the aging time of IGMP snooping queriers.
ip igmp snooping querier version	Specify the version of an IGMP snooping querier
ip igmp snooping query-max-response-time	Configure the maximum response time for Query packets.
ip igmp snooping source-check default-server	Enable the source IP address check function and specify the source IP address.
ip igmp snooping source-check port	Enable the source port check function.
ip igmp snooping suppression enable	Enable the Report packet suppression function.
ip igmp snooping svgl	Enable IGMP snooping globally and run the Shared VLAN Group Learning (SVGL) mode.
ip igmp snooping svgl profile	Specify the range of multicast groups applied in the SVGL mode.
ip igmp snooping svgl subvlan	Specify the sub VLANs applied in the SVGL mode.
ip igmp snooping svgl vlan	Specify the shared VLAN applied in the SVGL mode.
ip igmp snooping tunnel	Enable the function of transparent IGMP packet transmission on the QinQ port.
ip igmp snooping vlan	Enable the IGMP snooping function in IVGL mode on a VLAN.
ip igmp snooping vlan mrouter interface	Configure a static multicast router port.
ip igmp snooping vlan static interface	Configure a static member port.
permit	Permit a range of multicast groups defined by a profile.
range	Define a range of multicast groups for a profile.
show ip igmp profile	Display configurations of a profile.

show ip igmp snooping	Display IGMP snooping information.
show ip igmp snooping gda-table	Display the IGMP snooping forwarding table.
show ip igmp snooping interfaces	Display multicast filter configurations on a port.
show ip igmp snooping mrouter	Display IGMP snooping multicast router ports.
show ip igmp snooping querier	Display IGMP snooping querier information.
show ip igmp snooping statistics	Display IGMP snooping statistics.

1.1 clear ip igmp snooping gda-table

Function

Run the **clear ip igmp snooping gda-table** command to clear dynamic forwarding entries.

Syntax

clear ip igmp snooping gda-table

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

An Internet Group Management Protocol (IGMP) snooping forwarding entry includes the virtual local area network (VLAN) ID, multicast group address, multicast router ports, and member ports.

A VLAN ID (VID) and multicast group address uniquely identify a forwarding entry.

A forwarding entry may contain multiple multicast router ports, which may be dynamically learned or statically configured. Static multicast router ports never age.

A forwarding entry may contain multiple member ports, which may be dynamically learned or statically configured. Static member ports never age. This command cannot be used to delete static member ports.

Examples

The following example clears IGMP snooping dynamic forwarding entries.

```
Hostname> enable
Hostname# clear ip igmp snooping gda-table
```

Notifications

N/A

Platform Description

N/A

1.2 clear ip igmp snooping statistics

Function

Run the **clear ip igmp snooping statistics** command to clear IGMP snooping statistics.

Syntax

clear ip igmp snooping statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command can be used to clear statistics displayed by running the **show ip igmp snooping querier**

Function

Run the **show ip igmp snooping querier** command to display IGMP snooping querier information.

Syntax

show **ip igmp snooping querier** [**detail** | **vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IGMP snooping querier information.

```
Hostname# enable
Hostname# show ip igmp snooping querier
Vlan     IP Address          IGMP Version          Port
-----------------------------------------------------------
3        1.1.1.1               1                switch
```

Table 1-1 Output Fields of the show ip igmp snooping querier Command

Field	Description
Vlan	VLAN ID
IP Address	IP address
IGMP Version	IGMP version

Field	Description
Port	Port

Notifications

N/A

Platform Description

N/A

show ip igmp snooping statistics command.

Examples

The following example clears IGMP snooping statistics.

```
Hostname> enable
Hostname# clear ip igmp snooping statistics
```

Notifications

N/A

Platform Description

N/A

1.3 deny

Function

Run the **deny** command to deny a range of multicast groups specified by a profile.

The **deny** action is performed for a profile by default.

Syntax

deny

Parameter Description

N/A

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ip igmp profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

Examples

The following example creates profile 1, defines the group range of 224.2.2.2 to 224.2.2.244, and denies profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp profile**
- **range**
- **permit**
- **show ip igmp profile**

1.4 ip igmp profile

Function

Run the **ip igmp profile** command to create a profile and enter the profile configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No profile is created by default.

Syntax

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

default ip igmp profile *profile-number*

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ip igmp profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

(4) If the Deny action is configured and no multicast group range is configured, no group is denied. The effect is same as that of permitting all groups.

(5) If the Permit action is configured and no multicast group range is configured, no group is permitted. The effect is same as that of denying all groups.

Examples

The following example creates profile 1, defines the group range of 224.2.2.2 to 224.2.2.244, and permits profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **deny**
- **permit**
- **range**
- **show ip igmp profile**

1.5 ip igmp snooping dyn-mr-aging-time

Function

Run the **ip igmp snooping dyn-mr-aging-time** command to configure the aging time of dynamic multicast router ports.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default aging time of dynamic multicast router ports is 300s.

Syntax

ip igmp snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

no ip igmp snooping dyn-mr-aging-time

default ip igmp snooping dyn-mr-aging-time

Parameter Description

dynamic-mroute-aging-time: Aging time of dynamic router ports, in seconds. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If a dynamic multicast router port does not receive a general IGMP Query packet or a Protocol Independent Multicast (PIM) Hello packet before the aging time expires, the device deletes the port from the multicast router port list.

When the dynamic multicast router port learning function is enabled, you can run this command to adjust the aging time of dynamic multicast router ports. A too short aging time may cause multicast router ports to be added and deleted frequently.

Examples

The following example sets the aging time of dynamic multicast router ports to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping dyn-mr-aging-time 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.6 ip igmp snooping fast-leave enable

Function

Run the **ip igmp snooping fast-leave enable** command to enable the port fast leave function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The port fast leave function is disabled by default.

Syntax

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

default ip igmp snooping fast-leave enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the port fast leave function is enabled and a port receives a Leave packet, the port is directly deleted from the member port list of the corresponding multicast forwarding entry. When receiving group-specific Query packets, the device does not forward the packets to this port. Leave packets include IGMPv2 Leave packets and IGMPv3 Report packets of the INCLUDE type without carrying any source address.

The port fast leave function is applicable when only one host is connected to each port. This function helps save bandwidth and resources.

Examples

The following example enables the port fast leave function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping fast-leave enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.7 ip igmp snooping filter

Function

Run the **ip igmp snooping filter** command to apply a profile to a port to restrict the multicast groups that user hosts connecting to the port can join.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No profile is applied to a port by default.

Syntax

ip igmp snooping filter *profile-number*

no ip igmp snooping filter

default ip igmp snooping filter

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To specify a profile in the **ip igmp snooping filter** command, you must first create the profile.

After this command is configured on a port and the port receives a Report packet from a user host, the device checks whether the multicast address that the user host wants to join is within the multicast group range allowed by the profile. If yes, the user host can join the group. If no, the user host is not allowed to join the group.

Examples

The following example applies profile 1 to port GigabitEthernet 0/1 to restrict the multicast groups that user hosts connecting to the port can join.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ip igmp snooping filter 1
```

Notifications

When the configured profile does not exist, the following notification will be displayed:

```
% Error: Configure vlan filter fail
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**
- **show ip igmp snooping interfaces**

1.8 ip igmp snooping vlan filter

Function

Run the **ip igmp snooping vlan filter** command to apply a profile to a VLAN to restrict the multicast groups that user hosts in the VLAN can join.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No profile is applied to a VLAN by default.

Syntax

ip igmp snooping vlan *vlan-id* **filter** *profile-number*

no ip igmp snooping vlan *vlan-id* **filter**

default ip igmp snooping vlan *vlan-id* **filter**

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To specify a profile in the **ip igmp snooping vlan filter** command, you must first create the profile.

After this command is configured on a VLAN and the VLAN receives a Report packet from a user host, the device checks whether the multicast address that the user host wants to join is within the multicast group range allowed by the profile. If yes, the user host can join the group. If no, the user host is not allowed to join the group.

Examples

The following example applies profile 1 to VLAN 1 to restrict the multicast groups that the user hosts in the VLAN can join.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping vlan 1 filter 1
```

Notifications

When the configured profile does not exist, the following notification will be displayed:

```
% Error: Configure vlan filter fail
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**
- **show ip igmp snooping interfaces**

1.9 ip igmp snooping host-aging-time

Function

Run the **ip igmp snooping host-aging-time** command to configure the aging time for IGMP snooping dynamic member ports.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default aging time of IGMP dynamic member ports is 260s.

Syntax

ip igmp snooping host-aging-time *host-aging-time*

no ip igmp snooping host-aging-time

default ip igmp snooping host-aging-time

Parameter Description

host-aging-time: Aging time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device running IGMP snooping receives an IGMP Join packet from a host to join an IP multicast group, the device adds the port receiving the packet to the member port list and sets an aging time for the port.

If the port is already in the member port list, the device resets the aging timer of the port. The timer time is *host-aging-time*. After the timer times out, it is deemed that no user host receives multicast packets through this port, and the multicast device deletes the port from the IGMP snooping member port list. After this command is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent IGMP Join packets. The configured aging time takes effect after the next Join packet is received, and the started member port aging timers are not updated.

Examples

The following example sets the aging time of IGMP dynamic member ports to 30s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping host-aging-time 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.10 ip igmp snooping ivgl

Function

Run the **ip igmp snooping ivgl** command to enable IGMP snooping globally and run the Independent VLAN Group Learning (IVGL) mode.

Run the **no** form of this command to disable IGMP snooping.

Run the **default** form of this command to restore the default configuration.

IGMP snooping is disabled by default.

Syntax

ip igmp snooping ivgl

no ip igmp snooping

default ip igmp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In IVGL mode, multicast streams in different VLANs are independent of each other. A host can request only a multicast router port in the same VLAN to receive multicast data. Upon receiving multicast data in any VLAN, the device running IGMP snooping forwards the data only to member ports in the same VLAN.

Examples

The following example enables IGMP snooping and runs the IVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping ivgl
```

Notifications

When the device does not support the IVGL mode, the following notification will be displayed:

```
% Error: It’s invalid to configure IVGL mode in this product.
```

When L2 static multicast flow control is configured on the device, the following notification will be displayed, asking you to disable L2 static multicast flow control first:

```
% Error: IGMP Snooping conflicts with ip multicast static rule, please disable ip multicast static rule and try again.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.11 ip igmp snooping ivgl-svgl

Function

Run the **ip igmp snooping ivgl-svgl** command to enable IGMP snooping globally and run the IVGL-SVGL mode.

Run the **no** form of this command to disable IGMP snooping.

Run the **default** form of this command to restore the default configuration.

IGMP snooping is disabled by default.

Syntax

ip igmp snooping ivgl-svgl

no ip igmp snooping

default ip igmp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In IVGL-SVGL mode, the IVGL and SVGL modes coexist. A profile must be used to define a range of multicast groups applied in SVGL mode. Multicast data in this range applies to the SVGL mode, and other multicast data applies to the IVGL mode.

Note

The IVGL-SVGL mode is exclusive from the IP multicast function. If you want to enable IP multicast, please select the IVGL mode.

Examples

The following example enables IGMP snooping and runs the IVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping ivgl
```

The following example enables IGMP snooping and runs the IVGL-SVGL mode, sets the shared VLAN to VLAN 1, and sets the range of multicast groups applied in SVGL mode to Profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# permit
Hostname(config-profile)# range 224.1.1.1 238.1.1.1
Hostname(config-profile)# exit
Hostname(config)# ip igmp snooping ivgl-svgl
Hostname(config)# ip igmp snooping svgl profile 1
```

Notifications

When L2 static multicast flow control is configured on the device, the following notification will be displayed, asking you to disable L2 static multicast flow control first:

```
% Error: IGMP Snooping conflicts with ip multicast static rule, please disable ip multicast static rule and try again.
```

When the device does not support the SVGL mode, the following notification will be displayed:

```
% Error: It's invalid to configure SVGL mode in this product.
```

When the device enables the L3 IPv4 multicast routing function and does not support the configuration of SVGL mode, the following notification will be displayed:

```
% Error: You must disable ip multicast-routing first.
```

If no SVGL profile is configured when the SVGL mode is enabled, the following notification will be displayed:

```
% Warning: Please remember to configure SVGL profile
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp snooping svgl subvlan**
- **ip igmp snooping svgl vlan**
- **ip igmp snooping svgl**
- **show ip igmp snooping**

1.12 ip igmp snooping l2-entry-limit

Function

Run the **ip igmp snooping l2-entry-limit** command to configure the maximum number of multicast groups allowed for concurrent request globally.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of multicast groups allowed for concurrent request globally is **64000** by default.

Syntax

ip igmp snooping l2-entry-limit *l2-entry-limit*

no ip igmp snooping l2-entry-limit

default ip igmp snooping l2-entry-limit

Parameter Description

l2-entry-limit: Maximum number of multicast groups. The value range is from 0 to 65536.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The global maximum number of multicast groups allowed for concurrent request indicates groups on all ports in all VLANs and includes dynamically learned and statically configured multicast groups. When the number of multicast groups reaches the limit, learning new group records or configuring new static multicast group member ports are not allowed.

Examples

The following example sets the maximum number of multicast groups allowed for concurrent request globally to **2000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping l2-entry-limit 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.13 ip igmp snooping limit-ipmc vlan address server

Function

Run the **ip igmp snooping limit-ipmc vlan address server** command to specify a multicast group address and multicast source address for a VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Only the multicast source address is specified by default.

Syntax

ip igmp snooping limit-ipmc vlan *vlan-id* **address** *group-address* **server** *source-address*

no ip igmp snooping limit-ipmc vlan *vlan-id* **address** *group-address*

default ip igmp snooping limit-ipmc vlan *vlan-id* **address** *group-address*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

group-address: Multicast group address.

source-address: Multicast source address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source IP address check function and IP multicast routing function are mutually exclusive.

The source IP address check function is used to restrict the source IP address of multicast traffic. After the source IP address check function is enabled, multicast traffic with invalid multicast source address will be discarded.

To configure the source IP address check function, perform the following steps:

(1) Enable the source IP address check function and specify the multicast source address.

(2) (Optional) Specify a multicast group address and multicast source address for a specific VLAN.

Examples

The following example enables the source IP address check function to allows hosts in VLAN 203 and VLAN 204 to receive multicast traffic only from the source IP address of 192.168.1.10 and multicast group address of 229.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 203-204
Hostname(config-vlan-range)# exit
Hostname(config)# ip igmp snooping source-check default-server 192.168.1.11
Hostname(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
192.168.1.10
Hostname(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
```

Notifications

When the set source IP address is the same as the address of default source IP address check, the following notification will be displayed:

```
% Error: Please reset the limit ipmc ip address,because it's equal to the default source
ip
```

If the default source IP address check function is not enabled, the following notification will be displayed:

```
% Warning: Remember to configure source-ip check ability!
```

Common Errors

- The source IP address check function is not enabled.
- The source IP address specified in **ip igmp snooping limit-ipmc** is the same as the source IP address specified in **ip igmp snooping source-check default-server**.

Platform Description

N/A

Related Commands

N/A

1.14 ip igmp snooping max-groups

Function

Run the **ip igmp snooping max-groups** command to configure the maximum number of multicast groups that can be dynamically learned by a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of multicast groups that can be dynamically learned by a port is 64,000 by default.

Syntax

ip igmp snooping max-groups *max-groups*

no ip igmp snooping max-groups

default ip igmp snooping max-groups

Parameter Description

max-groups: Maximum number of multicast groups. The value range is from 0 to 64000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured and the number of multicast groups dynamically learned by a port exceeds the limit, the device no longer learns IGMP Report packets over this port to create new forwarding entries.

The number of multicast groups that can be dynamically learned by a port is counted based on the VLANs to which the port belongs. For example, if a port belongs to three VLANs and the port receives requests of multicast group 224.1.1.1 from each VLAN, the number of multicast groups dynamically learned by the port is 3 instead of 1.

Examples

The following example sets the maximum number of multicast groups that can be dynamically learned by GigabitEthernet 0/1 to **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ip igmp snooping max-group 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping interfaces**

1.15 ip igmp snooping mrouter learn pim-dvmrp

Function

Run the **ip igmp snooping mrouter learn pim-dvmrp** command to enable the function of dynamic multicast router port learning.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Dynamic multicast router port learning is enabled by default.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **mrouter learn pim-dvmrp**

no ip igmp snooping [**vlan** *vlan-id*] **mrouter learn pim-dvmrp**

default ip igmp snooping [**vlan** *vlan-id*] **mrouter learn pim-dvmrp**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The value range is from 1 to 4094. If this parameter is not specified, the dynamic multicast router port learning function is enabled or disabled for all VLANs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A multicast router port directly connects an IGMP snooping-enabled multicast device to a neighbor multicast device in which a multicast routing protocol is enabled. By default, when the dynamic multicast router port learning function is enabled, the device automatically listens to IGMP Query/DVMRP/PIM Hello packets and dynamically identifies multicast router ports.

To dynamically learn multicast router ports, enable the dynamic multicast router port learning function.

To configure static multicast router ports, run the **ip igmp snooping vlan mrouter interface** command.

To disable the dynamic multicast router port learning function for all VLANs, run the **no ip igmp snooping mrouter learn pim-dvmrp** command.

To disable the dynamic multicast router port learning function for a specific VLAN, run the **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp** command.

When the source port check function is enabled, only multicast traffic from the multicast router ports is valid and the multicast device forwards the traffic to registered ports. Multicast data from non-multicast router ports is invalid and will be discarded.

Examples

The following example enables dynamic multicast router port learning only on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip igmp snooping mrouter learn pim-dvmrp
Hostname(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.16 ip igmp snooping preview

Function

Run the **ip igmp snooping preview** command to enable the multicast preview function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The multicast preview function is disabled by default.

Syntax

ip igmp snooping preview *profile-number*

no ip igmp snooping preview

default ip igmp snooping preview

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the multicast preview function is enabled, a user who doesn't have access permission to certain multicast traffic (namely the user filtered out by IGMP snooping filter) can preview partial content of the multicast traffic. A profile is used to define the range of multicast groups allowed for preview.

The multicast preview function must be used in conjunction with IGMP snooping filter or multicast control.

Examples

The following example enables the multicast preview function (with profile 1 applied) to be used together with IGMP snooping filter (with profile 2 applied) configured on GigabitEthernet.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping preview 1
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ip igmp snooping filter 2
```

Notifications

When the configured profile does not exist, the following notification will be displayed:

```
% Error: The profile doesn't exist, Please configure it first of all
```

Common Errors

IGMP snooping filter or multicast control is not used to control permissions of multicast groups.

Platform Description

N/A

Related Commands

N/A

1.17 ip igmp snooping preview interval

Function

Run the **ip igmp snooping preview interval** command to configure the multicast preview duration.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default multicast preview duration is 60s.

Syntax

ip igmp snooping preview interval *preview-interval*

no ip igmp snooping preview interval

default ip igmp snooping preview interval

Parameter Description

preview-interval: Multicast preview duration, in seconds. The value range is from 1 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the multicast preview function and sets the preview duration to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping preview 1
Hostname(config)# ip igmp snooping preview interval 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip igmp snooping querier

Function

Run the **ip igmp snooping querier** command to enable the IGMP snooping querier function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The IGMP snooping querier function is disabled by default.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier**

no ip igmp snooping [**vlan** *vlan-id*] **querier**

default ip igmp snooping [**vlan** *vlan-id*] **querier**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, the IGMP snooping querier function is enabled or disabled for all VLANs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To activate the IGMP querier function on a VLAN, you must enable the function globally and then enable it on the VLAN.

If the IGMP snooping querier function is disabled globally, the function is disabled on all VLANs.

Examples

The following example enables the IGMP querier function on VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier
Hostname(config)# ip igmp snooping vlan 2 querier
```

Notifications

When the IGMP querier function is enabled on a VLAN before it is enabled globally, the following notification will be displayed:

```
% Command did not take effect due to reason: IGMP switch querier is globally disabled
```

Common Errors

The IGMP querier function is enabled on a VLAN before it is enabled globally. As a result, the IGMP querier function on the VLAN does not take effect.

Platform Description

N/A

Related Commands

N/A

1.19 ip igmp snooping querier address

Function

Run the **ip igmp snooping querier address** command to configure the source IP address of the IGMP snooping querier.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The source IP address configuration applies to all VLANs by default.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier address** *source-address*

no ip igmp snooping [**vlan** *vlan-id*] **querier address**

default ip igmp snooping [**vlan** *vlan-id*] **querier address**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The querier source IP address configured on a specific VLAN, if any, prevails.

source-address: Source IP address of the querier.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the querier function is enabled, you must specify a source IP address for the querier so that the querier function can take effect.

The querier source IP address configured on a specific VLAN, if any, prevails.

Examples

The following example sets the source IP address of the IGMP snooping querier to **1.1.1.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier address 1.1.1.1
```

The following example sets the source IP address of the IGMP snooping querier on VLAN 3 to **1.1.1.1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 3
Hostname(config-vlan)# exit
Hostname(config)# ip igmp snooping vlan 3 querier address 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip igmp snooping querier max-response-time

Function

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of IGMP snooping queriers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum response time of IGMP snooping queriers is 10s by default.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier max-response-time** *max-response-time*

no ip igmp snooping [**vlan** *vlan-id*] **querier max-response-time**

default ip igmp snooping [**vlan** *vlan-id*] **querier max-response-time**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The maximum response time configured on a specific VLAN, if any, prevails.

max-response-time: Maximum response time of queriers, in seconds. The value range is from 1 to 25.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The maximum response time configured on a specific VLAN, if any, prevails.

Examples

The following example sets the maximum response time of queriers to 15s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier max-response-time 15
```

The following example sets the maximum response time of queriers on VLAN 3 to 15s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 3
Hostname(config-vlan)# exit
Hostname(config)# ip igmp snooping vlan 3 querier max-response-time 15
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip igmp snooping querier query-interval

Function

Run the **ip igmp snooping querier query-interval** command to configure the interval for an IGMP snooping querier to send Query packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default interval for an IGMP snooping querier to send Query packets is 60s.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier query-interval** *query-interval*

no ip igmp snooping [**vlan** *vlan-id*] **querier query-interval**

default ip igmp snooping [**vlan** *vlan-id*] **querier query-interval**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The query interval configured on a specific VLAN, if any, prevails.

query-interval: Interval for a querier to send Query packets, in seconds. The value range is from 1 to 18000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The query interval configured on a specific VLAN, if any, prevails.

Examples

The following example sets the query interval to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier query-interval 100
```

The following example sets the query interval on VLAN 3 to 100s.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# vlan 3
Hostname(config-vlan)# exit
Hostname(config)# ip igmp snooping vlan 3 querier query-interval 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip igmp snooping querier timer expiry

Function

Run the **ip igmp snooping querier timer expiry** command to configure the aging time of IGMP snooping queriers.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default aging time of IGMP snooping queriers is 125s.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier timer expiry** *timeout*

no ip igmp snooping [**vlan** *vlan-id*] **querier timer expiry**

default ip igmp snooping [**vlan** *vlan-id*] **querier timer expiry**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The querier aging time configured on a specific VLAN, if any, prevails.

timeout: Aging time of a querier, in seconds. The value range is from 60 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the IGMP querier function is enabled and multiple queriers are configured in the network, querier election will be performed. The device elected as the querier will send Query packets periodically. Other candidate queriers receive Query packets from the elected querier. If a candidate querier does not receive Query packets

from the elected querier within a specific period of time, the candidate querier regards that it is the only querier in the directly-connected network segment and initiates a new round querier election.

The querier aging time configured on a specific VLAN, if any, prevails.

Examples

The following example sets the querier aging time to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier timer expiry 60
```

The following example sets the querier aging time on VLAN 3 to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 3
Hostname(config-vlan)# exit
Hostname(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ip igmp snooping querier version

Function

Run the **ip igmp snooping querier version** command to specify the version of an IGMP snooping querier

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default version of an IGMP snooping querier is **version 2**.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **querier version** { **1** | **2** }

no ip igmp snooping [**vlan** *vlan-id*] **querier version**

default ip igmp snooping [**vlan** *vlan-id*] **querier version**

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The IGMP snooping querier version configured on a specific VLAN, if any, prevails.

1: Specifies IGMPv1.

2: Specifies IGMPv2.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An IGMP snooping querier supports IGMPv1, IGMPv2, and IGMPv3.

The IGMP snooping querier version configured on a specific VLAN, if any, prevails.

Examples

The following example sets the IGMP snooping querier version to IGMPv1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping querier version 1
```

The following example sets the IGMP snooping querier version on VLAN 3 to IGMPv1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 3
Hostname(config-vlan)# exit
Hostname(config)# ip igmp snooping vlan 3 querier version 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ip igmp snooping query-max-response-time

Function

Run the **ip igmp snooping query-max-response-time** command to configure the maximum response time for Query packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum response time for Query packets is 10s by default.

Syntax

ip igmp snooping query-max-response-time *query-max-response-time*

no ip igmp snooping query-max-response-time

default ip igmp snooping query-max-response-time

Parameter Description

query-max-response-time: Maximum response time for Query packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When receiving group-specific Query packets, the multicast device will reset the aging timers of all dynamic member ports of this multicast group. The timer time is *query-max-aging-time*. After the timer times out, it is deemed that no user host receives multicast packets through this port, and the multicast device deletes the port from the IGMP snooping member port list.

The configured aging time takes effect after the next Query packet is received, and the started aging timers are not updated. For IGMPv3 group-specific Query packets, the multicast device does not update the timers.

Examples

The following example sets the maximum response time for Query packets to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping query-max-response-time 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ip igmp snooping source-check default-server

Function

Run the **ip igmp snooping source-check default-server** command to enable the source IP address check function and specify the source IP address.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Source IP address check is disabled by default.

Syntax

ip igmp snooping source-check default-server *source-address*

no ip igmp snooping souce-check

default ip igmp snooping souce-check

Parameter Description

source-address: Multicast source IP address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source IP address check function and IP multicast routing function are mutually exclusive.

The source IP address check function is used to restrict the source IP address of multicast traffic. After the source IP address check function is enabled, multicast traffic with invalid multicast source address will be discarded.

To configure the source IP address check function, perform the following steps:

(1) Enable the source IP address check function and specify the multicast source address.

(2) (Optional) Specify a multicast group address and multicast source address for a specific VLAN.

Examples

The following example enables the source IP address check function to allow hosts in VLAN 203 and VLAN 204 to receive multicast traffic only from the source IP address 192.168.1.10 and multicast group address 229.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 203-204
Hostname(config-vlan-range)# exit
Hostname(config)# ip igmp snooping source-check default-server 192.168.1.10
Hostname(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
192.168.1.10
```

```
Hostname(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
```

Notifications

When the set default source IP address is the same as that specified in the **ip igmp snooping limit-ipmc** command, the following notification will be displayed:

```
% Error: The default-server address is conflict!
```

When the L3 multicast routing function is enabled, the following notification will be displayed:

```
% Error: You must disable multicast-routing first
```

If the device does not support the source IP address check function, the following notification will be displayed:

```
% Error: Switch does not support source-ip check!
```

Common Errors

The source IP address specified in **ip igmp snooping source-check default-server** is the same as the source IP address specified in **ip igmp snooping limit-ipmc**.

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.26 ip igmp snooping source-check port

Function

Run the **ip igmp snooping source-check port** command to enable the source port check function.

Run the **no** form of this command to disable this function.

Run the **default** form of this port command to restore the default configuration.

Source port check is disabled by default.

Syntax

ip igmp snooping source-check port

no ip igmp snooping source-check port

default ip igmp snooping source-check port

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source port check function is used to restrict multicast traffic to be forwarded only through multicast router ports. After this function is enabled, only multicast traffic received on multicast router ports is valid. Multicast traffic received on other ports is invalid and will be discarded. If no multicast router port exists in a VLAN, multicast traffic in the VLAN will be discarded.

When the source port check function is disabled, multicast traffic received on any port is valid and will be forwarded to the corresponding member ports.

Examples

The following example enables the source port check function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping source-check port
```

Notifications

If the device does not support the source port check function, the following notification will be displayed:

```
% Error: Source-port check is invalid in this product
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.27 ip igmp snooping suppression enable

Function

Run the **ip igmp snooping suppression enable** command to enable the Report packet suppression function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Report packet suppression is disabled by default.

Syntax

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

default ip igmp snooping suppression enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When Report packet suppression is enabled, the IGMP multicast device forwards only the first Report packet from a specific VLAN for a multicast group to the multicast router port and suppresses subsequent Report packets for the same multicast group during one query interval. This function helps reduce the number of packets in the network.

Only IGMPv1 and IGMPv2 Report packets can be suppressed, and IGMPv3 Report packets cannot be suppressed.

Examples

The following example enables the Report packet suppression function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping suppression enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.28 ip igmp snooping svgl

Function

Run the **ip igmp snooping svgl** command to enable IGMP snooping globally and run the Shared VLAN Group Learning (SVGL) mode.

Run the **no** form of this command to disable IGMP snooping.

Run the **default** form of this command to restore the default configuration.

IGMP snooping is disabled by default.

Syntax

ip igmp snooping svgl

no ip igmp snooping

default ip igmp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In SVGL mode, hosts in different VLANs share multicast data. Hosts can request multicast data across VLANs. A shared VLAN (VLAN 1 by default) needs to be designated. Only multicast data in the shared VLAN can be forwarded to all member ports of the group address. These member ports can be in other VLANs. A profile must be used to define a range of multicast groups applied in SVGL mode. Only multicast data from this range can be forwarded across VLANs, and other multicast data will be discarded.

Note

The SVGL mode is exclusive from the IP multicast function. If you want to enable IP multicast, please select the IVGL mode.

Examples

The following example enables IGMP snooping and runs the SVGL mode, sets the shared VLAN to VLAN 1, and sets the range of multicast groups applied in SVGL mode to Profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# permit
Hostname(config-profile)# range 224.1.1.1 238.1.1.1
Hostname(config-profile)# exit
Hostname(config)# ip igmp snooping svgl
Hostname(config)# ip igmp snooping svgl profile 1
```

Notifications

When L2 static multicast flow control is configured on the device, the following notification will be displayed, asking you to disable L2 static multicast flow control first:

```
% Error: IGMP Snooping conflicts with ip multicast static rule, please disable ip multicast static rule and try again.
```

When the device does not support the SVGL mode, the following notification will be displayed:

```
% Error: It's invalid to configure SVGL mode in this product.
```

When the device enables the L3 IPv4 multicast routing function and does not support the configuration of SVGL mode, the following notification will be displayed:

```
% Error: You must disable ip multicast-routing first.
```

If no SVGL profile is configured when the SVGL mode is enabled, the following notification will be displayed:

```
% Warning: Please remember to configure SVGL profile
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp snooping svgl subvlan**
- **ip igmp snooping svgl vlan**
- **show ip igmp snooping**

1.29 ip igmp snooping svgl profile

Function

Run the **ip igmp snooping svgl profile** command to specify the range of multicast groups applied in the SVGL mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No multicast group is associated with the SVGL mode by default.

Syntax

ip igmp snooping svgl profile *profile-number*

no ip igmp snooping svgl profile

default ip igmp snooping svgl profile

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the device running IGMP snooping operates in SVGL or IVGL-SVGL mode, the multicast groups associated with the SVGL mode must be configured.

First, define the multicast groups applied in the SVGL mode in a profile. Then, apply this profile in this command.

Examples

The following example applies profile 2 to the SVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#ip igmp profile 2
Hostname(config-profile)#permit
Hostname(config-profile)#range 225.1.1.1 225.1.255.255
Hostname(config-profile)#exit
Hostname(config)# ip igmp snooping svgl profile 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp profile**
- **show ip igmp snooping**

1.30 ip igmp snooping svgl subvlan

Function

Run the **ip igmp snooping svgl subvlan** command to specify the sub VLANs applied in the SVGL mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All VLANs except the shared VLAN are sub VLANs in SVGL mode by default.

Syntax

ip igmp snooping svgl subvlan [*vlan-range*]

no ip igmp snooping svgl subvlan [*vlan-range*]

default ip igmp snooping svgl subvlan [*vlan-range*]

Parameter Description

vlan-range: VLAN ID or VLAN ID range. *vlan-range* can be set to a single VLAN or a range of VLANs. When a range of VLANs is configured, use commas (,) to separate VIDs. Consecutive VIDs can also be connected using hyphens (-). There is no sequence requirement for the VIDs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device running IGMP snooping operates in SVGL or IVGL-SVGL mode, you can run this command to configure the multicast groups associated with the SVGL mode.

Examples

The following example sets the shared VLAN to VLAN 3 and sub VLANs to VLANs 2, 5, 6, and 7 for the SVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-3,5-7
Hostname(config-vlan-range)# exit
Hostname(config)# ip igmp snooping svgl vlan 3
Hostname(config)# ip igmp snooping svgl subvlan 2,5-7
```

Notifications

When the number of configured sub VLANs exceeds the limit 127, the following notification will be displayed:

```
% Error: Reach max subvlan entries than what allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp snooping svgl vlan**

1.31 ip igmp snooping svgl vlan

Function

Run the **ip igmp snooping svgl vlan** command to specify the shared VLAN applied in the SVGL mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default shared VLAN is VLAN 1.

Syntax

ip igmp snooping svgl vlan *vlan-id*

no ip igmp snooping svgl vlan

default ip igmp snooping svgl vlan

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device running IGMP snooping operates in SVGL or IVGL-SVGL mode, you can run this command to configure the shared VLAN applied in the SVGL mode.

Examples

The following example sets the shared VLAN to VLAN 3 and sub VLANs to VLANs 2, 5, 6, and 7 for the SVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-3,5-7
Hostname(config-vlan-range)# exit
Hostname(config)# ip igmp snooping svgl vlan 3
Hostname(config)# ip igmp snooping svgl subvlan 2,5-7
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp snooping svgl subvlan**
- **show ip igmp snooping**

1.32 ip igmp snooping tunnel

Function

Run the **ip igmp snooping tunnel** command to enable the function of transparent IGMP packet transmission on the QinQ port.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of transparent IGMP packet transmission on the QinQ port is disabled by default.

Syntax

ip igmp snooping tunnel

no ip igmp snooping tunnel

default ip igmp snooping tunnel

Parameter Description

N/A

Default Level

14

Command Modes

Global configuration mode

Usage Guidelines

On a device with IGMP snooping enabled and a dot1q-tunnel (QinQ) port configured, IGMP snooping will process the IGMP packets received on the QinQ port using the following two modes:

- Mode 1: Transmit IGMP packets in transparent mode on the QinQ port. Create multicast entries on the VLAN where the IGMP packets are located and forward IGMP packets on the VLAN. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the IGMP Report packet to the multicast router port of VLAN 10.
- Mode 2: Create multicast entries on the default VLAN of the QinQ port. Encapsulate the IGMP packets with the VLAN tag of the default VLAN where the QinQ port is located and forward the packets within the default VLAN. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the IGMP Report packet with the tag of VLAN 1, and forwards the packet to the multicast router port of VLAN 1.

IGMP snooping works in mode 2 by default.

Examples

The following example enables the function of transparent IGMP packet transmission on the QinQ port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping tunnel
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**
-

1.33 ip igmp snooping vlan

Function

Run the **ip igmp snooping vlan** command to enable the IGMP snooping function in IVGL mode on a VLAN.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

If the IGMP snooping function in IVGL mode is enabled globally, the function is enabled on all VLANs.

If the IGMP snooping function in IVGL mode is disabled globally, the function is disabled on all VLANs.

Syntax

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

default ip igmp snooping vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the IGMP snooping function in IVGL mode is enabled globally, you can run the **no ip igmp snooping vlan** *vlan-id* command to enable the IGMP snooping function in IVGL mode on VLANs except the specified VLAN.

Examples

The following example enables the IGMP snooping function in IVGL mode globally and disables the function on VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping ivgl
Hostname(config)# no ip igmp snooping vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping vlan**

1.34 ip igmp snooping vlan mrouter interface

Function

Run the **ip igmp snooping vlan mrouter interface** command to configure a static multicast router port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static multicast router port is configured by default.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

no ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

default ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

interface-type interface-number: Interface name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To dynamically learn multicast router ports, enable the dynamic multicast router port learning function, which is enabled by default.

To configure static multicast router ports, run the **ip igmp snooping vlan mrouter interface** command. Static multicast router ports never age.

If a port is configured as a static multicast router port, the device can forward all received multicast traffic over this port.

When the source port check function is enabled, only multicast traffic from the multicast router ports is valid and the multicast device forwards the traffic to registered ports. Multicast data from non-multicast router ports is invalid and will be discarded.

Examples

The following example configures GigabitEthernet 0/1 in VLAN 1 as a static multicast router port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/1
```

Notifications

When a static multicast router port fails to be configured, the following notification will be displayed:

```
% Error: Configure this interface static multicast route failure
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**
-

1.35 ip igmp snooping vlan static interface

Function

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static member port is configured by default.

Syntax

ip igmp snooping vlan *vlan-id* **static** *group-address* **interface** *interface-type interface-number*

no ip igmp snooping vlan *vlan-id* **static** *group-address* **interface** *interface-type interface-number*

default ip igmp snooping vlan *vlan-id* **static** *group-address* **interface** *interface-type interface-number*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

group-address: Multicast group address.

interface-type interface-number: Interface name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An IGMP snooping forwarding entry includes the VLAN ID, multicast group address, multicast router ports, and member ports.

A VID and multicast group address uniquely identify a forwarding entry.

A forwarding entry may contain multiple multicast router ports, which may be dynamically learned or statically configured. Static multicast router ports never age.

A forwarding entry may contain multiple member ports, which may be dynamically learned or statically configured. Static member ports never age. The **clear ip igmp snooping gda-table** command cannot be used to delete static member ports.

Examples

The following example establishes a forwarding entry and sets the VLAN ID to 1, multicast group address to 224.1.1.1, and static member port to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface gigabitethernet
0/1
```

Notifications

When a static member port fails to be configured, the following notification will be displayed:

```
% Error: Configure static multicast group in this port fail
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip igmp snooping**

1.36 permit

Function

Run the **permit** command to permit a range of multicast groups defined by a profile.

The **deny** action is performed for a profile by default.

Syntax

permit

Parameter Description

N/A

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ip igmp profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups. The default action is **deny**.

Examples

The following example permits multicast groups in the range of 224.2.2.2 to 224.2.2.244 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **deny**
- **ip igmp profile**
- **range**
- **show ip igmp profile**

1.37 range

Function

Run the **range** command to define a range of multicast groups for a profile.

Run the **no** form of this command to remove this configuration.

No multicast group range is defined for a profile by default.

Syntax

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter Description

low-ip-address: Start IP address of a multicast group range.

high-ip-address: End IP address of a multicast group range.

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ip igmp profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups. The default action is **deny**.

Examples

The following example permits multicast groups in the range of 224.2.2.2 to 224.2.2.244 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **deny**
- **ip igmp profile**

- **permit**
- **show ip igmp profile**

1.38 show ip igmp profile

Function

Run the **show ip igmp profile** command to display configurations of a profile.

Syntax

show ip igmp profile [*profile-number*]

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024. If this parameter is not configured, configurations of all profiles are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about configured profiles.

Examples

The following example displays information about configured profiles.

```
Hostname> enable
Hostname# show ip igmp profile
PROFILE    1
       DENY
       RANGE 224.1.1.1,   225.1.1.1
```

Table 1-2 Output Fields of the show ip igmp profile Command

Field	Description
PROFILE	Profile ID.
PERMIT/DENY	Run the **permit** or **deny** command to permit or deny a range of multicast groups. The default action is **deny**.
RANGE	Range of multicast groups defined in a profile.

Notifications

N/A

Platform Description

N/A

1.39 show ip igmp snooping

Function

Run the **show ip igmp snooping** command to display IGMP snooping information.

Syntax

show ip igmp snooping [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IGMP snooping status and parameters globally or on a specific VLAN.

Examples

The following example displays IGMP snooping information globally.

```
Hostname> enable
Hostname# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 64000
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

Table 1-3 Output Fields of the show ip igmp snooping Command

Field	Description
IGMP Snooping running mode	IGMP snooping working mode ● IVGL mode: provides independent multicast services for each user VLAN. ● SVGL mode: provides shared multicast services for user VLANs. ● IVGL-SVGL mode: provides both shared and independent multicast services for user VLANs.
IGMP Snooping L2-entry-limit	Global maximum number of multicast groups allowed for concurrent request
Source port check	Source port check
Source ip check	Source IP address check
IGMP Fast-Leave	Port fast leave
IGMP Report suppress	Report packet suppression
IGMP Globle Querier	Global IGMP snooping querier
IGMP Preview	IGMP multicast preview
IGMP Tunnel	Transparent IGMP packet transmission on the QinQ port
IGMP Snooping version	IGMP snooping version
IGMP Preview group aging time	IGMP multicast preview duration
Dynamic Mroute Aging Time	Aging time of dynamic multicast router ports
Dynamic Host Aging Time	Aging time of dynamic member ports

The following example displays IGMP snooping information on VLAN 1.

```
Hostname> enable
Hostname# show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Respone Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
vlan 1
----
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
```

```
IGMP Fast-Leave: Disable
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

Table 1-4 Output Fields of the show ip igmp snooping vlan Command

Field	Description
IGMP Snooping running mode	IGMP snooping working mode ● IVGL mode: provides independent multicast services for each user VLAN. ● SVGL mode: provides shared multicast services for user VLANs. ● IVGL-SVGL mode: provides both shared and independent multicast services for user VLANs.
IGMP Snooping L2-entry-limit	Global maximum number of multicast groups allowed for concurrent request
Global IGMPv2 Fast-Leave	Global port fast leave
Global multicast router learning mode	Global dynamic multicast router port learning ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Query Max Respone Time	Maximum response time of an IGMP snooping querier
Dynamic Mroute Aging Time	Aging time of dynamic multicast router ports
Dynamic Host Aging Time	Aging time of dynamic member ports
vlan	Specified VLAN
IGMP Snooping state	IGMP snooping status
Multicast router learning mode	Dynamic multicast router port learning on a specified VLAN
IGMP Fast-Leave	Fast leave of a member port on a specific VLAN
IGMP VLAN querier	IGMP snooping querier of a specific VLAN
IGMP VLAN Mode	VLAN mode ● **STATIC**: static mode ● **DYNAMIC**: dynamic mode ● **PRIVATE**: private VLAN mode ● **SUPER**: VLAN aggregation mode

Notifications

N/A

Platform Description

N/A

1.40 show ip igmp snooping gda-table

Function

Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table.

Syntax

show ip igmp snooping gda-table

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the IGMP snooping forwarding table.

```
Hostname# enable
Hostname# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.1.1, 20):
  VLAN(20) 3 OPORTS:
    ROUTER(M)
    GigabitEthernet 0/23(D)
    GigabitEthernet 0/24(M)
```

Table 1-5 Output Fields of the show ip igmp snooping gda-table Command

Field	Description
D: DYNAMIC	Dynamic member port
S: STATIC	Static member port
M: MROUTE	Multicast router port
(*, *group-address*, *vlan-id*)	Multicast entry ● *: any source ● group-address: Multicast group address ● *vlan-id*: VLAN ID

Field	Description
VLAN(*vlan-id*) *oport-number* OPORTS	*oport-number* outbound ports under VLAN *vlan-id*
ROUTER(M)	Multicast router port of the local device
interface-type interface-number (D)	Dynamic member port
interface-type interface-number (M)	Multicast router port

Notifications

N/A

Platform Description

N/A

1.41 show ip igmp snooping interfaces

Function

Run the **show ip igmp snooping interfaces** command to display multicast filter configurations on a port.

Syntax

show ip igmp snooping interfaces [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays multicast filter configurations on GigabitEthernet 0/1.

```
Hostname# enable
Hostname# show ip igmp snooping interfaces GigabitEthernet 0/1
      Interface            Filter profile number       max-group
-------------------------     ---------------------       ---------
GigabitEthernet 0/1                                  1000
```

Table 1-6 Output Fields of the show ip igmp snooping interfaces Command

Field	Description
Interface	Interface
Filter profile number	Profile ID
max-group	Maximum number of multicast groups that can be dynamically learned by a port

Notifications

N/A

Platform Description

N/A

1.42 show ip igmp snooping mrouter

Function

Run the **show ip igmp snooping mrouter** command to display IGMP snooping multicast router ports.

Syntax

show ip igmp snooping mrouter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IGMP snooping multicast router ports.

```
Hostname# enable
Hostname# show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 2):
  VLAN(2)  1 MROUTES:
    GigabitEthernet 0/23(D)
```

Table 1-7 Output Fields of the show ip igmp snooping mrouter Command

Field	Description
D: DYNAMIC	Dynamic multicast router port
S: STATIC	Static multicast router port
(*, *, *vlan-id*):	(Multicast source, multicast group, VLAN)
VLAN(*vlan-id*) *mroute-interface-number* MROUTES	*Mroute-interface-number* multicast router ports under VLAN *vlan-id*
interface-type interface-number (D)	Dynamic multicast router port

Notifications

N/A

Platform Description

N/A

1.43 show ip igmp snooping querier

Function

Run the **show ip igmp snooping querier** command to display IGMP snooping querier information.

Syntax

s**how ip igmp snooping querier** [**detail** | **vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IGMP snooping querier information.

```
Hostname# enable
Hostname# show ip igmp snooping querier
Vlan     IP Address         IGMP Version         Port
-----------------------------------------------------------
```

```
3       1.1.1.1              1               switch
```

Table 1-8 Output Fields of the show ip igmp snooping querier Command

Field	Description
Vlan	VLAN ID
IP Address	IP address
IGMP Version	IGMP version
Port	Port

Notifications

N/A

Platform Description

N/A

1.44 show ip igmp snooping statistics

Function

Run the **show ip igmp snooping statistics** command to display IGMP snooping statistics.

Syntax

show ip igmp snooping statistics [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IGMP snooping statistics.

```
Hostname# enable
Hostname# show ip igmp snooping statistics

Current number of Gda-table entries: 0
Configured Statistics database limit: 64000
```

```
Current number of IGMP Query packet received: 0
Current number of IGMPv1/v2 Report packet received: 0
Current number of IGMPv3 Report packet received: 0
Current number of Leave packet received: 0
Current number of PIM packet received: 0
Current number of DVMRP packet received: 0
Current number of SQL Exec waited: 0
```

Table 1-9 Output Fields of the show ip igmp snooping statistics Command

Field	Description
Current number of Gda-table entries	Number of IGMP snooping forwarding entries
Configured Statistics database limit	Maximum number of multicast entries
Current number of IGMP Query packet received	Number of IGMP Query packets received
Current number of IGMPv1/v2 Report packet received	Number of IGMPv1/IGMPv2 Report packets received
Current number of IGMPv3 Report packet received	Number of IGMPv3 Report packets received
Current number of Leave packet received	Number of Leave packets received
Current number of PIM packet received	Number of PIM packets received
Current number of DVMRP packet received	Number of DVMRP packets received
Current number of SQL Exec waited	Number of SQL statements waiting for execution

Notifications

N/A

Platform Description

N/A

1 MSDP Commands

Command	Function
clear ip msdp peer	Reset the TCP connection with an MSDP peer and clear statistics about the MSDP peer.
clear ip msdp sa-cache	Clear the SA cache entries.
clear ip msdp statistics	Clear statistics about an MSDP peer.
ip msdp default-peer	Configure a default MSDP peer.
ip msdp description	Add description information for an MSDP peer.
ip msdp filter-sa-request	Filter SA request messages from an MSDP peer.
ip msdp mesh-group	Add an MSDP peer to a mesh group.
ip msdp originator-id	Configure the primary address of a specified interface as the initiator address in SA messages.
ip msdp password peer	Enable the MD5 authentication function on the TCP connection with an MSDP peer.
ip msdp peer connect-source	Add an MSDP peer.
ip msdp redistribute	Control the (S, G) information released on an MSDP device.
ip msdp sa-filter in	Configure an incoming filter of SA messages.
ip msdp sa-filter out	Configure an outgoing filter of SA messages.
ip msdp sa-limit	Define the maximum number of SA cache entries from an MSDP peer.
ip msdp shutdown	Disable the connection with an MSDP peer.
ip msdp timer	Configure a TCP reconnection interval.
ip msdp ttl-threshold	Define the time to live (TTL) value of the multicast packets in SA messages.
ip msdp peer-limit	Define the number of MSDP peers supported on a device.
ip msdp global-sa-limit	Define the SA cache capacity supported on a device.

show ip msdp count	Display the number of sources and number of groups in SA messages and the number of SA cache entries from MSDP peers.
show ip msdp mesh-group	Display the information of a mesh group.
show ip msdp peer	Display detailed information about an MSDP peer.
show ip msdp rpf-peer	Display the MSDP RPF peer information corresponding to the address of a specified initiator.
show ip msdp sa-cache	Display the learned (S, G) information.
show ip msdp sa-originated	Display the (S, G) information that meets the redistribution filtering rule and is initiated by the local device.
show ip msdp summary	Display summary information of all MSDP peers.

1.1 clear ip msdp peer

Function

Run the **clear ip msdp peer** command to reset the TCP connection with an MSDP peer and clear statistics about the MSDP peer.

Syntax

clear ip msdp peer *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

"Reset" means canceling and then re-establishing the TCP connection with the MSDP peer.

Examples

The following example resets the TCP connection with the MSDP peer 218.14.5.23 and clears statistics about this MSDP peer.

```
Hostname> enable
Hostname# clear ip msdp peer 218.14.5.23
```

Notifications

N/A

Platform Description

N/A

1.2 clear ip msdp sa-cache

Function

Run the **clear ip msdp sa-cache** command to clear the SA cache entries.

Syntax

clear ip msdp sa-cache [*ipv4-group-address*]

Parameter Description

ipv4-group-address: Address of an IPv4 multicast group.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear the SA cache entries learned from MSDP peers. If no multicast group address is specified, all SA cache entries are cleared.

After the SA cache entries are cleared, the MSDP device needs to re-learn SA messages.

Examples

The following example clears SA cache entries learned from the multicast group 224.1.1.1.

```
Hostname> enable
Hostname# clear ip msdp sa-cache 224.1.1.1
```

Notifications

N/A

Platform Description

N/A

1.3 clear ip msdp statistics

Function

Run the **clear ip msdp statistics** command to clear statistics about an MSDP peer.

Syntax

clear ip msdp statistics [*ipv4-peer-address*]

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to refresh the statistics about an MSDP peer without resetting the TCP connection with the MSDP peer, including MSDP peer information, resetting information, and I/O information.

Examples

The following example clears the statistics about the MSDP peer 61.83.1.52.

```
Hostname> enable
Hostname# clear ip msdp statistics 61.83.1.52
```

Notifications

N/A

Platform Description

N/A

1.4 ip msdp default-peer

Function

Run the **ip msdp default-peer** command to configure a default MSDP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No default MSDP peer is configured by default.

Syntax

ip msdp default-peer *ipv4-peer-address* [**prefix-list** *prefix-list-name*]

no ip msdp default-peer *ipv4-peer-address*

default ip msdp default-peer *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

prefix-list *prefix-list-name*: Specifies a prefix list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

SA messages from MSDP peers may fail the peer RPF check and then be discarded. If an MSDP peer is configured as a default MSDP peer, SA messages from this MSDP peer pass the peer RPF check.

If the **prefix-list** keyword parameter is not specified, all SA messages are accepted.

If an inexistent **prefix-list** is specified, all SA messages are accepted.

If an existent **prefix-list** is specified, only the SA messages of RPs specified in this prefix list are accepted.

Examples

The following example configures the MSDP peer 172.16.33.1 as a default peer.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 172.16.33.1 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp peer 172.16.34.2 connect-source gigabitethernet 0/2
Hostname(config)# ip msdp default-peer 172.16.33.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip prefix-list** (IP routing/routing policy)
- **ip msdp peer connect-source**

1.5 ip msdp description

Function

Run the **ip msdp description** command to add description information for an MSDP peer.

Run the **no** form of command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No description information is added for an MSDP peer by default.

Syntax

ip msdp description *ipv4-peer-address description*

no ip msdp description *ipv4-peer-address*

default ip msdp description *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

description: Description information. It is a string of 1 to 256 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The administrator can add description information for MSDP peers so that the MSDP peers can be distinguished with ease.

If description information A is specified for an MSDP peer, the description information of the MSDP peer is displayed as "A".

If no description information is specified for an MSDP peer, the description information of the MSDP peer is displayed as "No description".

Examples

The following example adds customer-a as the description information of the peer 172.17.1.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 172.171.1.2 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp description 172.171.1.2 customer-a
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp peer**

1.6 ip msdp filter-sa-request

Function

Run the **ip msdp filter-sa-request** command to filter SA request messages from an MSDP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All SA request messages from MSDP peers are received and replied by default.

Syntax

ip msdp filter-sa-request *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* }]

no ip msdp filter-sa-request *ipv4-peer-address*

default ip msdp filter-sa-request *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

list *acl-name*: Uses an IP standard ACL name to define the address range of multicast groups. The value is a case-sensitive string of 1 to 99 characters.

list *acl-number*: Uses an IP standard ACL number to define the address range of multicast groups. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **list** keyword parameter is not specified, all the SA request messages are ignored.

If the **list** keyword parameter is specified but this ACL is not configured, all SA request messages are ignored.

If the **list** keyword parameter is specified and this ACL is configured, only the SA request messages allowed by the ACL are accepted, and other SA request messages are ignored.

Examples

The following example uses ACL 1 that defines the valid address range of multicast groups as 224.0.1.0/24 to filter SA request messages from the peer 172.16.223.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 172.16.223.1 connect-source gigabitethernet 0/1
Hostname(config)# access-list 1 permit 224.0.1.1 0.0.0.255
Hostname(config)# ip msdp filter-sa-request 172.16.223.1 list 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp sa-cache**

1.7 ip msdp mesh-group

Function

Run the **ip msdp mesh-group** command to add an MSDP peer to a mesh group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No mesh group is configured and no MSDP peer is added to any mesh group by default.

Syntax

ip msdp mesh-group *mesh-name ipv4-peer-address*

no ip msdp mesh-group *mesh-name ipv4-peer-address*

default ip msdp mesh-group *mesh-name ipv4-peer-address*

Parameter Description

mesh-name: Name of a mesh group. The value is a case-sensitive string of 1 to 256 characters.

ipv4-peer-address: IPv4 address of an MSDP peer.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An MSDP peer relationship must be established between every two MSDP peers in the same mesh group.

SA messages from members of a mesh group can pass the peer RPF check.

SA messages from a mesh group member are not forwarded to the other members in the same mesh group.

Examples

The following example adds the MSDP peer 192.168.1.3 to a mesh group MSDP-Mesh.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 192.168.1.3 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp mesh-group msdp-mesh 192.168.1.3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp mesh-group**

1.8 ip msdp originator-id

Function

Run the **ip msdp originator-id** command to configure the primary address of a specified interface as the initiator address in SA messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no primary address of an interface is specified as the initiator address of SA messages.

Syntax

ip msdp originator-id *interface-type interface-number*

no ip msdp originator-id

default ip msdp originator-id

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command configures the primary address of an interface as the initiator address in SA messages. If no IP address is configured for this interface or this interface is down, the RP address configured with PIM, other than the primary IP address of this interface, is used as the initiator address in SA messages.

In anycast RP deployment mode, this command must be used to modify the initiator address in SA messages.

Examples

The following example configures the IP address of Loopback0 as the initiator address in SA messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface loopback 0
Hostname(config-if-Loopback 0)# exit
Hostname(config)# ip msdp originator-id loopback 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip msdp password peer

Function

Run the **ip msdp password peer** command to enable the MD5 authentication function on the TCP connection with an MSDP peer.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The MD5 authentication function is disabled by default.

Syntax

ip msdp password peer *ipv4-peer-address* [*encryption-type*] *password-string*

no ip msdp password peer *ipv4-peer-address*

default ip msdp password peer *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

encryption-type: Encryption level. The value is 0 or 7, and the default value is **0**. A larger value means a higher encryption level.

password-string: Cypher used for TCP MD5 authentication. If the encryption level is 0, a cypher can consist of 80 characters at most. If the encryption level is 7, a cypher can consist of 160 characters at most.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To authenticate the ID of an MSDP peer, enable MD5 authentication on the TCP connection established with this MSDP peer. The MSDP peers must have the consistent configuration, and the cipher must be the same; otherwise, the connection fails.

If the configuration or cipher changes, the local device does not stop the current session, and attempts to use a new cipher to retain the current session until timeout.

Note

- If the encryption level is 0, the key set for TCP connection is the original key entered from the console. That is, Ruijie devices with encryption level 0 can match devices of any other vendor with encryption level 0. When MSDP devices of Ruijie Networks interact with MSDP devices of another vendor and authentication is needed, encryption level 0 is used.
- If the encryption level is 7, the key set for TCP connection is not the original key entered from the console. The original key string is calculated using the key algorithms of Ruijie Networks to obtain a new key string. And then, the new key string is set for TCP connection. Therefore, encryption level 7 boasts higher security. Encryption level 7 of Ruijie Networks is supported on any Ruijie device. However, devices of Ruijie Networks may not interact with devices of any other vendor in this case. This is because the key algorithms of each vendor are private and not publicized.
- If the encryption level is specified as 7, the length of the entered ciphertext string must be an even number equal to or greater than four.

Examples

The following example configures the MD5 cypher of TCP connection with the peer 10.32.43.144 as test.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 10.32.43.144 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp password peer 10.32.43.144 0 test
```

Notifications

If MD5 authentication is enabled on the local device but not enabled on the MSDP peer, the following notification will be displayed:

```
%TCP-BADAUTH: MD5 digest NOT expected but found (200.200.200.6,
39996)->(200.200.200.16, 639)
```

If the MD5 cypher configured on the local device is inconsistent with that configured on the MSDP peer, the following notification will be displayed:

```
%TCP-BADAUTH: MD5 digest failed for (200.200.200.6, 12302)->(200.200.200.16, 639)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp summary**

1.10 ip msdp peer connect-source

Function

Run the **ip msdp peer connect-source** command to add an MSDP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No MSDP peer is added by default.

Syntax

ip msdp peer *ipv4-peer-address* **connect-source** *interface-type interface-number*

no ip msdp peer *ipv4-peer-address*

default ip msdp peer *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer. The MSDP peer uses this IPv4 address to establish a TCP connection with the local device.

interface-type interface-number: Type and number of a local interface. A loopback interface is recommended. The local device uses the primary IPv4 address of this interface to establish a TCP connection with the MSDP peer. If no IPv4 address is configured for this interface or the interface is down, the MSDP peer relationship cannot be established.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A TCP connection is established between the local device and the MSDP peer.

This command configures the connection only on the local device. The same settings must be configured on the MSDP peer.

Examples

The following example uses the IP address of loopback 0 to establish an MSDP peer relationship with 192.168.5.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface loopback 0
Hostname(config-if-Loopback 0)# exit
Hostname(config)# ip msdp peer 192.168.5.1 connect-source loopback 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip msdp peer**
- **show ip msdp summary**

1.11 ip msdp redistribute

Function

Run the **ip msdp redistribute** command to control the (S, G) information released on an MSDP device.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All (S, G) information registered on the local RP is released on the MSDP device by default.

Syntax

ip msdp redistribute [{ **list** *acl-name* | **list** *acl-number* } | **route-map** *route-map-name*] *

no ip msdp redistribute

default ip msdp redistribute

Parameter Description

list *acl-name*: Uses an IP extended ACL name to define the valid address range of (S, G) information. The value is a case-sensitive string of 1 to 99 characters.

list *acl-number*: Uses an IP extended ACL number to define the valid address range of (S, G) information. The value range is from 100 to 199 or from 2000 to 2699.

route-map *route-map-name*: Uses a route map to define the valid address range of (S, G) information.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **ip msdp redistribute** command is also referred to as redistribution filter. After this command is configured, only allowed (S, G) information of the local or other domains can pass filtering on the MSDP device.

- If the **list** keyword parameter is specified, only the (S, G) information matching this ACL is released.
- If the **route-map** keyword parameter is specified, only the (S, G) information matching this route map is released.
- If both the parameters are specified, only the (S, G) information matching the ACL and route map is released.
- If no parameter is specified, no (S, G) information is released.

The methods of associating the redistribution filter with the route map are as follows:

- If the applied *route-map* does not exist, all multicast source information is filtered out.
- If BGP is not enabled on the local device, all multicast source information is filtered out.

Based on the optimal route, the AS path of a specified address is calculated. For the address of an external AS, the AS path is obtained based on the optimal route. For the address of a local AS, an AS path that includes the local AS is constructed. The AS path result is filtered based on the route map applied to the AS path.

The local device is RP on which BGP is enabled and the AS number is set to 100. The route map associated with redistribution is named re-route-map. To enable multicast source information to be redistributed in the local AS, include the AS path matching rule of the local AS in the route map. Some configuration of the route map and AS path ACL is as follows:

```
route-map re-route-map permit 10
match as-path 1
ip as-path access-list 1 permit 100
```

Examples

The following example uses ACL 100 to define the (S, G) information that can pass filtering by an MSDP device and sets the address range of the multicast source to 200.200.200.0/24 and the address range of the multicast group to 225.1.1.0/24.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip access-list extended 100
Hostname(config-ext-nacl)# permit ip 200.200.200.0 0.0.0.255 225.1.1.0 0.0.0.255
Hostname(config)# ip msdp redistribute list 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip msdp sa-cache**
- **show ip msdp sa-originated**

1.12 ip msdp sa-filter in

Function

Run the **ip msdp sa-filter in** command to configure an incoming filter of SA messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All SA messages from MSDP peers are received by default.

Syntax

ip msdp sa-filter in *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* } | **route–map** *route-map-name* | { **rp-list** *acl-name* | **rp-list** *acl-number* } | **rp-route-map** *rp-route-map-name*] *

no ip msdp sa-filter in *ipv4-peer-address*

default ip msdp sa-filter in *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

list *acl-name*: Uses an IP extended ACL name to define the (S, G) information that can pass filtering. The value is a case-sensitive string of 1 to 99 characters.

list *acl- number*: Uses an IP extended ACL number to define the (S, G) information that can pass filtering. The value range is from 100 to 199 or from 2000 to 2699.

route-map *route-map-name*: Specifies the route map name of (S, G) information. The (S, G) information can pass filtering only when the AS path of the source route matches the AS path of this route map.

rp-list *acl-name*: Uses an IP standard ACL name to define the RP range in the (S, G) information that can pass filtering. The value is a case-sensitive string of 1 to 99 characters.

rp-list *acl-number*: Uses an IP standard ACL number to define the RP range in the (S, G) information that can pass filtering. The value range is from 1 to 99.

rp-route-map *rp-route-map-name*: Specifies the route map name of an RP. The (S, G) information can pass filtering only when the AS path of the RP route matches the AS path of this route map.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If this command is configured, but no ACL or route map is specified, all incoming SA messages are filtered out.

If only one keyword (**list** or **route-map**) is specified and the (S, G) information in an SA message meets the rule specified by the keyword, the (S, G) is received.

If only one keyword (**rp-list** or **rp-route-map**) is specified and the RP address in an SA message meets the rule specified by this keyword, this SA message is received.

If two or more of the keywords (including **list**, **route-map, rp-list**, and **rp-route-map**) are specified and the (S, G) information in an SA message meets the rules specified by all the keywords, this SA message is received.

The methods of associating the incoming SA message filter with the route map are as follows:

(1) If the applied *route-map* does not exist, all multicast source information is filtered out.

(2) If BGP is not enabled on the local device, all multicast source information is filtered out.

(3) Based on the optimal route, the AS path of a specified address is calculated. For the address of an external AS, the AS path is obtained based on the optimal route. For the address of a local AS, an AS path that includes the local AS is constructed. The AS path result is filtered based on the route map applied to the AS path.

Examples

The following example filters all SA messages from the peer 10.234.1.43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 10.234.1.43 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp sa-filter in 10.234.1.43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp sa-cache**

1.13 ip msdp sa-filter out

Function

Run the **ip msdp sa-filter out** command to configure an outgoing filter of SA messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, all SA messages are forwarded to MSDP peers.

Syntax

ip msdp sa-filter out *ipv4-peer-address* [**list** { *acl-name* | *acl-number* } | **route–map** *route-map-name* | **rp-list** { *acl-name* | *acl-number* } | **rp-route-map** *rp-route-map*] *

no ip msdp sa-filter out *ipv4-peer-address*

default ip msdp sa-filter out *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

list *acl-name*: Uses an IP extended ACL name to define the (S, G) information that can pass filtering. The value is a case-sensitive string of 1 to 99 characters.

list *acl- number*: Uses an IP extended ACL number to define the (S, G) information that can pass filtering. The value range is from 100 to 199 or from 2000 to 2699.

route-map *route-map-name*: Specifies the route map name of (S, G) information. The (S, G) information can pass filtering only when the AS path of the source route matches the AS path of this route map.

rp-list *acl-name*: Uses an IP standard ACL name to define the RP range in the (S, G) information that can pass filtering. The value is a case-sensitive string of 1 to 99 characters.

rp-list *acl-number*: Uses an IP standard ACL number to define the RP range in the (S, G) information that can pass filtering. The value range is from 1 to 99.

rp-route-map *rp-route-map-name*: Specifies the route map name of an RP. The (S, G) information can pass filtering only when the AS path of the RP route matches the AS path of this route map.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If this command is configured, but no ACL or route map is specified, no SA message is sent to this MSDP peer.

If only one of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) is specified and the (S, G) information in an SA message meets the rule specified by this keyword, this SA message is forwarded to this MSDP peer.

If two or more of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) are specified and the (S, G) information in an SA message meets the rules specified by these keywords, this SA message is forwarded to this MSDP peer.

The methods of associating the outgoing SA message filter with the route map are as follows:

(1) If the applied *route-map* does not exist, all multicast source information is filtered out.

(2) If BGP is not enabled on the local device, all multicast source information is filtered out.

(3) Based on the optimal route, the AS path of a specified address is calculated. For the address of an external AS, the AS path is obtained based on the optimal route. For the address of a local AS, an AS path that includes the local AS is constructed. The AS path result is filtered based on the route map applied to the AS path.

Examples

The following example uses ACL 100 to define the multicast source information sent to the peer 10.234.1.43, and sets the address range of the multicast source to 10.211.0.0/16 and the address range of the multicast group to 224.12.0.0/16.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 100 permit ip 10.211.0.0 0.0.255.255 224.12.0.0
0.0.255.255
Hostname(config)# ip msdp peer 10.234.1.43 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp sa-filter out 10.234.1.43 list 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**
- **show ip msdp sa-cache**

1.14 ip msdp sa-limit

Function

Run the **ip msdp sa-limit** command to define the maximum number of SA cache entries from an MSDP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of SA cache entries from an MSDP peer is not specified by default.

Syntax

ip msdp sa-limit *ipv4-peer-address sa-limit*

no ip msdp sa-limit *ipv4-peer-address*

default ip msdp sa-limit *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

sa-limit: Maximum number of SA cache entries. The value range is from 1 to 4096.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is configured to prevent SA message flooding from an MSDP peer.

After the local device learns A SA entries from an MSDP peer and the maximum number of SA cache entries set for this MSDP peer is B, if the value of A is greater than that of B, the SA entries learned from this MSDP peer are not cleared immediately. Rather, the number of SA entries automatically drops to B based on the SA entry aging mechanism (no more than 135 seconds). This command does not take effect immediately, and it is used to retain valid multicast source information as much as possible and improve the network efficiency. To immediately clear the SA entries from this MSDP peer, you can use this command together with the **clear ip msdp sa-cache** command.

Examples

The following example sets the limit of SA entries from the MSDP peer 172.16.3.1 to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 172.16.3.1 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp sa-limit 172.16.3.1 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**

- **show ip msdp sa-cache**

1.15 ip msdp shutdown

Function

Run the **ip msdp shutdown** command to disable the connection with an MSDP peer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The connection with an MSDP peer is enabled by default.

Syntax

ip msdp shutdown *ipv4-peer-address*

no ip msdp shutdown *ipv4-peer-address*

default ip msdp shutdown *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command disables only the TCP connection with an MSDP peer, but does not delete this MSDP peer or clear configuration of this MSDP peer.

Examples

The following example disables the connection with the MSDP peer 192.168.7.20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp shutdown 192.168.7.20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip msdp summary**

1.16 ip msdp timer

Function

Run the **ip msdp timer** command to configure a TCP reconnection interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default TCP reconnection interval is **30** seconds.

Syntax

ip msdp timer *interval*

no ip msdp timer

default ip msdp timer

Parameter Description

interval: TCP reconnection interval, in seconds. The value range is from 1 to 60.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Within the TCP reconnection interval, the MSDP peer on the proactive connection side can initiate at most one TCP connection. In some application scenarios, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

Examples

The following example sets the TCP reconnection interval to 20 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp timer 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp shutdown**

1.17 ip msdp ttl-threshold

Function

Run the **ip msdp ttl-threshold** command to define the time to live (TTL) value of the multicast packets in SA messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The TTL value of the multicast packets in SA messages is not defined by default.

Syntax

ip msdp ttl-threshold *ipv4-peer-address ttl-value*

no ip msdp ttl-threshold *ipv4-peer-address*

default ip msdp ttl-threshold *ipv4-peer-address*

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

ttl-value: TTL value. The value range is from 0 to 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command controls the sending of multicast packets encapsulated in SA messages. A multicast packet is sent to the MSDP peer only when the TTL value in the IP header of the multicast packet is equal to or greater than the preset TTL threshold. If the TTL value in the IP header of the multicast packet is smaller than the preset TTL threshold, the multicast packet is removed from the SA message and discarded before the SA message is sent to the MSDP peer.

This command affects the sending of multicast packets in SA messages, and does not affect the sending of (S, G) information in the SA messages.

Examples

The following example sets the TTL value of the peer 192.168.10.1 to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer 192.168.10.1 connect-source gigabitethernet 0/1
Hostname(config)# ip msdp ttl-threshold 192.168.10.1 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip msdp peer connect-source**

1.18 ip msdp peer-limit

Function

Run the **ip msdp peer-limit** command to define the number of MSDP peers supported on a device.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of MSDP peers supported on a device is **64** by default.

Syntax

ip msdp peer-limit *peer-limit*

no ip msdp peer-limit

default ip msdp peer-limit

Parameter Description

peer-limit: Maximum number of MSDP peers supported on a device. The value range is from 1 to 128.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of MSDP peers supported on a device.

When this command is configured, if the number of MSDP peers on the device exceeds the value to be configured, a prompt message is displayed indicating configuration failure. You need to delete some peers to ensure that the configuration can succeed.

Examples

The following example sets the number of MSDP peers supported on a device to 128.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp peer-limit 128
```

Notifications

If the number of MSDP peers on the device exceeds the value to be configured, the configuration fails.

When the configured number of MSDP peers on a device is 80 and there are 85 MSDP peers existing on the device, the following notification will be displayed. In this case, you need to delete at least five MSDP peers to make the configuration succeed.

```
%% Current number of msdp peers(85) exceeds configured peer limit (80).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ip msdp global-sa-limit

Function

Run the **ip msdp global-sa-limit** command to define the SA cache capacity supported on a device.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default SA cache capacity supported on a device is **1024**.

Syntax

ip msdp global-sa-limit *sa-limit*

no ip msdp global-sa-limit

default ip msdp global-sa-limit

Parameter Description

sa-limit: SA cache capacity supported on a device. The value range is from 1 to 4096.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to adjust the SA cache capacity of a device. You are advised to configure this command when you start the device.

During MSDP running, if the capacity is increased, the adjustment does not affect the SA cache entries that are originally learned.

If the capacity is decreased, all SA cache entries learned and initiated must be deleted and re-learned.

Examples

The following example sets the SA cache capacity supported on a device to 4096.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip msdp global-sa-limit 4096
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ip msdp count

Function

Run the **show ip msdp count** command to display the number of sources and number of groups in SA messages and the number of SA cache entries from MSDP peers.

Syntax

show ip msdp count [*as-number*]

Parameter Description

as-number: AS number. The value range is from 1 to 4294967295.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the number of sources and number of groups in SA messages and the number of SA cache entries from MSDP peers.

```
Hostname> enable
Hostname# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
```

```
 1.1.1.2       : 0
 100.100.100.14 : 0
 100.100.100.15 : 0
 100.100.100.200: 0
 200.200.200.2  : 2
 200.200.200.3  : 0
 200.200.200.6  : 0
 200.200.200.13 : 0
 200.200.200.66 : 0
SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 2
100: 1/2
```

Table 1-1 Output Fields of the show ip msdp count Command

Field	Description
<Peer>:<# SA learned>	MSDP peer and SA entries learned from this MSDP peer. For example, "200.200.200.200 : 2" indicates that two SA entries are learned from the MSDP peer 200.200.200.200.
<asn>: <# sources>/<# groups>	RP AS and the number of sources and number of groups initiated by the RP. For example, "100 : 1/2" indicates that there are one multicast source and two multicast groups in the RP of AS 100.
Total entries	Number of all SA entries learned from all MSDP peers. For example, "Total entries: 2" indicates that the number of SA entries learned from all MSDP peers is 2.

Notifications

N/A

Platform Description

N/A

1.21 show ip msdp mesh-group

Function

Run the **show ip msdp mesh-group** command to display the information of a mesh group.

Syntax

show ip msdp mesh-group

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of a mesh group.

```
Hostname> enable
Hostname# show ip msdp mesh-group
MSDP peers in each Mesh-group, <Mesh-group name>:<# peers>
msdp-mesh:
  1.1.1.2
  1.1.1.3
```

Table 1-2 Output Fields of the show ip msdp mesh-group Command

Field	Description
<Mesh-group name>:<# peers>	Name of a mesh group and all MSDP peers in this mesh group. Example: msdp-mesh: 1.1.1.2 1.1.1.3 Indicates a mesh group msdp-mesh and the MSDP peers 1.1.1.2 and 1.1.1.3 in this mesh group.

Notifications

N/A

Platform Description

N/A

1.22 show ip msdp peer

Function

Run the **show ip msdp peer** command to display detailed information about an MSDP peer.

Syntax

show ip msdp peer [*ipv4-peer-address*]

Parameter Description

ipv4-peer-address: IPv4 address of an MSDP peer.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays detailed information about the MSDP peer 20.0.0.1.

```
Hostname> enable
Hostname# show ip msdp peer 20.0.0.1
MSDP PEER 20.0.0.1 (No description), AS unknown
 Connection status:
   State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2)
   Uptime(Downtime): 00:00:25, Message sent/received: 13/19
   Input messages discarded: 0
   Connection and counters cleared 00:13:25 ago
   Local Address of connection: 20.0.0.2
   MD5 signature protection on MSDP TCP connection: enabled
 SA Filtering:
   Input (S,G) Access-list filter: None
   Input (S,G) route-map filter: None
   Input RP Access-list filter: None
   Input RP Route-map filter: None
   Output (S,G) Access-list filter: None
   Output (S,G) Route-map filter: None
   Output RP Access-list filter: None
   Output RP Route-map filter: None
 SA-Requests:
   Input filter: None
 Peer ttl threshold: 0
 SAs learned from this peer: 2, SAs limit: No-limit
 Message counters:
   SA messages discarded: 0
   SA messages in/out: 13/0
   SA Requests discarded/in: 0/0
   SA Responses out: 0
   Data Packets in/out: 6/0
```

Table 1-3 Output Fields of the show ip msdp peer Command

Field	Description
MSDP Peer	IP address of an MSDP peer.
AS	AS of MSDP peers. If an AS is unknown, it is displayed as "unknown".
State	State of an MSDP peer.
Connection source	Source interface of a TCP connection and primary IP address of this interface. If no primary IP address is available to this interface, the primary IP address of this interface is displayed as "unknown".
MD5 signature protection on MSDP TCP connection: enabled	If MD5 authentication is enabled on the TCP connection with the MSDP peer, this field is displayed. Otherwise, this field is not displayed.
Peer is member of mesh-group MSDP	If the MSDP peer is added to a mesh group, this field is displayed. Otherwise, this field is not displayed.
Uptime(Downtime)	Uptime and downtime of the MSDP peer.
Messages sent/received	Number of SA messages sent/received to/from the MSDP peer.
SA Filtering	Incoming/Outgoing SA message filtering
SAs learned from this peer	SA messages learned from the MSDP peer.
SAs limit	Maximum number of SA cache entries of the MSDP peer.
Data Packets in/out	Multicast packets in incoming/outgoing SA messages.

Notifications

N/A

Platform Description

N/A

1.23 show ip msdp rpf-peer

Function

Run the **show ip msdp rpf-peer** command to display the MSDP RPF peer information corresponding to the address of a specified initiator.

Syntax

show ip msdp rpf-peer *ipv4-address*

Parameter Description

ipv4-address: IPv4 address of the initiator in an SA message.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the RPF peer information corresponding to the RP address 1.1.1.1.

```
Hostname> enable
Hostname# show ip msdp rpf-peer 1.1.1.1
RPF peer information for 1.1.1.1
RPF peer: 200.200.200.2
RPF rule: Peer is only active peer
RPF route/mask: Not-used
RPF type: Not-used
```

Table 1-4 Output Fields of the show ip msdp rpf-peer Command

Field	Description
RPF peer information for	RPF peer information corresponding to a specified RP address.
RPF peer	RPF peer address corresponding to a specified RP address.
RPF rule	Rule used to calculate the RPF peer corresponding to a specified RP address.
RPF route/mask	Network segment and mask corresponding to a specified RP address, used to determine the RPF peer. If the rule used to calculate the RPF peer corresponding to a specified RP address does not contain the routing information, this field is displayed as "Not-used", indicating that the network segment and mask corresponding to the RP address are not used. The rule used in the preceding example is "unique active MSDP peer". The route to the RP address is not used; therefore, this field is displayed as "Not-used".
RPF type	Routing protocol used to calculate the RPF peer corresponding to an RP address. If the rule used to calculate the RPF peer corresponding to a specified RP address does not contain the routing information, this field is displayed as "Not-used", indicating that the routing protocol is not used. The rule used in the preceding example is "unique active MSDP peer". The route to the RP address is not used; therefore, this field is displayed as "Not-used".

Notifications

N/A

Platform Description

N/A

1.24 show ip msdp sa-cache

Function

Run the **show ip msdp sa-cache** command to display the learned (S, G) information.

Syntax

show ip msdp sa-cache [*ipv4-group-address* | *ipv4-source-address*] [*ipv4-group-address* | *ipv4-source-address*] [*as-number*]

Parameter Description

ipv4-group-address: Address of an IPv4 multicast group.

ipv4- source-address: Address of an IPv4 multicast source.

as-number: Number of an AS in which SA messages are generated. The value range is from 1 to 4294967295.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified, all the (S, G) information is displayed by default.

If an address is specified, the device checks whether this address is a unicast or multicast address. If the address is a unicast address, this address is treated as the multicast source (S), and all (S, G) information in which the multicast source is S is displayed. If the address is a multicast address, this address is treated as the multicast group (G), and all (S, G) information in which the multicast group is G is displayed. If this address is neither a unicast nor a multicast address, no information is displayed.

If two addresses are specified, one address is treated as the multicast source (S), and the other as the multicast group (G). If one address is the unicast address, and the other address is the multicast group address, no information is displayed.

Examples

The following example displays the learned (S, G) information.

```
Hostname> enable
Hostname# show ip msdp sa-cache
MSDP Source-Active Cache: 2 entries
  (200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05,
Peer 200.200.200.2
```

```
   Learned from peer 200.200.200.2, RPF peer 200.200.200.2,
   SAs received: 277, Encapsulated data received: 0
  (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05,
Peer 200.200.200.2
   Learned from peer 200.200.200.2, RPF peer 200.200.200.2,
SAs received: 277, Encapsulated data received: 0
```

Table 1-5 Output Fields of the show ip msdp sa-cache Command

Field	Description
(200.200.200.200, 227.1.2.2)	Source address (first IP address) and group address (second IP address) in an SA message.
RP 20.20.20.20	RP address from which SA messages are generated.
(M)BGP/AS 100	RP AS in which SA messages are generated. The AS number is calculated based on MBGP or BGP. If the AS is unknown, it is displayed as "unknown".
04:17:09/00:02:05	Cache duration 4 hours, 17 minutes, and 9 seconds. If no local SA message is received within two minutes and five seconds, the cached SA message is deleted.
Peer 200.200.200.2	MSDP peer that this SA message comes from.
Learned from peer 200.200.200.2	MSDP peer that this SA message comes from.
RPF peer 200.200.200.2	RPF peer corresponding to the RP address from which this SA message is generated.
SAs received	Times of receiving this SA message.
Encapsulated data received	Times of encapsulating multicast data in this SA message.

Notifications

N/A

Platform Description

N/A

1.25 show ip msdp sa-originated

Function

Run the **show ip msdp sa-originated** command to display the (S, G) information that meets the redistribution filtering rule and is initiated by the local device.

Syntax

show ip msdp sa-originated

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If multicast source (S, G) information is registered on the local RP and the local RP is configured with an MSDP peer, you can run this command to display the (S, G) information initiated by this RP.

The (S, G) information displayed by this command has met the rule specified by the redistribution filtering command **ip msdp redistribute**. You can run the **ip msdp sa-filter out** command to check whether the (S, G) information meets the outgoing SA information filtering rule and can be initiated by MSDP peers.

Examples

The following example displays (S, G) information that is initiated by the local device and meets the redistribution filtering rule.

```
Hostname> enable
Hostname# show ip msdp sa-originated
MSDP Source-Active Originated: 5 entries
(192.168.23.78, 225.0.0.1), RP: 192.168.23.249
(192.168.23.79, 225.0.0.2), RP: 192.168.23.249
(192.168.23.80, 225.0.0.3), RP: 192.168.23.249
(192.168.23.81, 225.0.0.4), RP: 192.168.23.249
(192.168.23.82, 225.0.0.5), RP: 192.168.23.249
```

Table 1-6 Output Fields of the show ip msdp sa-originated Command

Field	Description
(192.168.23.78, 225.0.0.1)	Source address (first IP address) and group address (second IP address) from which SA messages are initiated.
RP 192.168.23.249	RP address from which SA messages are initiated.

Notifications

N/A

Platform Description

N/A

1.26 show ip msdp summary

Function

Run the **show ip msdp summary** command to display summary information of all MSDP peers.

Syntax

show ip msdp summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays summary information of all MSDP peers.

```
Hostname> enable
Hostname# show ip msdp summary
Msdp Peer Status Summary
Peer Address    As   State   Uptime/Downtime   Reset-Count   Sa-Count
Peer-description
200.200.200.2   100   Up     04:22:11         10           6616      No description
200.200.200.3   100   Down   19:17:13         4            0         peer-A
```

Table 1-7 Output Fields of the show ip msdp summary Command

Field	Description
Peer Address	IP address of MSDP peers.
AS	AS of MSDP peers.
State	State of MSDP peers.
Uptime/Downtime	Uptime and downtime of MSDP peers.
Reset-Count	Times of MSDP peer disconnections.
Sa-count	Number of SA messages received from this MSDP peer.
Peer-description	Description information of an MSDP peer. If no description information is specified for this MSDP peer, the description information of the MSDP peer is displayed as "No description".

Notifications

N/A

Platform Description

N/A

1 IPv6 Multicast Route Management Commands

Command	Function
clear ipv6 mroute	Clear IPv6 multicast hardware forwarding entries.
clear ipv6 mroute statistics	Clear statistics about the IPv6 multicast hardware forwarding entries.
ipv6 mroute	Configure an IPv6 static multicast route.
ipv6 multicast boundary	Configure an IPv6 multicast border for a specified IPv6 group.
ipv6 multicast route-limit	Configure the maximum number of entries in an IPv6 multicast routing table.
ipv6 multicast-routing	Enable the IPv6 multicast routing function.
ipv6 multicast rpf longest-match	Enable the function of RPF route selection based on the longest match rule.
ipv6 multicast static	Enable the multicast stream L2 direction control function.
msf6 force-forwarding	Enable the function of forced forwarding of IPv6 multicast packets (destined for the CPU) by software.
msf6 nsf	Enable the nonstop forwarding (NSF) function.
show ipv6 mroute	Display IPv6 multicast hardware forwarding entries.
show ipv6 mroute count	Display the count of IPv6 multicast routing entries.
show ipv6 mroute sparse	Display PIM-SMv6 multicast core entries.
show ipv6 mroute static	Display the IPv6 static multicast routing information.
show ipv6 mroute summary	Display the summary information of IPv6 multicast routing entries.
show ipv6 mvif	Display IPv6 multicast interface information.
show ipv6 rpf	Display the RPF information about a specific IPv6 source address.
show ipv6 mrf6 mfc	Display IPv6 multicast routing entries.
show msf6 msc	Display IPv6 L2/L3 multicast hardware forwarding entries.

show msf6 nsf	Display IPv6 multicast NSF configuration.

1.1 clear ipv6 mroute

Function

Run the **clear ipv6 mroute** command to clear IPv6 multicast hardware forwarding entries.

Syntax

clear ipv6 mroute { ***** | *ipv6-group-address* [*ipv6-source-address*] }

Parameter Description

*****: Clears all IPv6 multicast routing entries.

ipv6-group-address: Address of an IPv6 multicast group for IPv6 multicast routing.

ipv6-source-address: Address of an IPv6 multicast source for IPv6 multicast routing.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the multicast function fails, you can run this command to clear the current IPv6 multicast routing information to facilitate problem locating and re-learn entries.

Examples

The following example clears all the IPv6 multicast routing entries.

```
Hostname> enable
Hostname# clear ipv6 mroute *
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear ipv6 mroute statistics

Function

Run the **clear ipv6 mroute statistics** command to clear statistics about the IPv6 multicast hardware forwarding entries.

Syntax

clear ipv6 mroute statistics { ***** | *ipv6-group-address* [*ipv6-source-address*] }

Parameter Description

*****: Specifies all IPv6 multicast routing entries.

ipv6-group-address: Address of an IPv6 multicast group for IPv6 multicast routing.

ipv6-source-address: Address of an IPv6 multicast source for IPv6 multicast routing.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the multicast function fails, you can run this command to clear the current multicast routing statistics to facilitate problem locating and re-collect information.

Examples

The following example clears statistics about all the IPv6 multicast routing entries.

```
Hostname> enable
Hostname# clear ipv6 mroute statistics *
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ipv6 mroute

Function

Run the **ipv6 mroute** command to configure an IPv6 static multicast route.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IPv6 static multicast route is configured by default.

Syntax

ipv6 mroute *ipv6-address/prefix-length* [*protocol*] { *ipv6-rpf-address* | *interface-type interface-number* } [*distance*]

no ipv6 mroute *ipv6-address/prefix-length* [*protocol*]

default ipv6 mroute *ipv6-address/prefix-length* [*protocol*]

Parameter Description

ipv6-address: IPv6 address of a multicast source.

prefix-length: Mask of the IPv6 address of a multicast source.

protocol: Unicast routing protocol being used.

ipv6-rpf-address: IPv6 address of an RPF neighbor (next hop to the multicast source).

interface-type interface-number: RPF interface (outbound interface to the multicast source).

distance: Route administrative distance. The value range is from 0 to 255, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A static multicast route is used for only RPF check, and specifies an RPF neighbor or interface for multicast packets from a specific source. A static multicast route is applied in mainly the following two scenarios:

- Modify an RPF route

  If a multicast device expects to receive multicast packets from a source through a specified interface but this specified interface is not the RPF interface, you can configure a static multicast route to specify this interface as an RPF interface.

- Connect an RPF route

  If two adjacent devices in a network are configured with different routing protocols, and the routes are not mutually introduced, the unicast route is interrupted. The devices cannot forward packets because no RPF route is available. In this case, you can configure a static multicast route to specify the RPF interface to complete the RPF check and implement multicast packet forwarding.

To specify an outbound interface rather than a next-hop IP address for the IPv6 static multicast route, ensure that the outbound interface is of the point-to-point type.

Examples

The following example configures an IPv6 static multicast route, and sets the network address of the IPv6 multicast to 2233::/64 and the outbound interface address of this multicast source to 3333::3333.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mroute 2233::/64 3333::3333
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mroute static**

1.4 ipv6 multicast boundary

Function

Run the **ipv6 multicast boundary** command to configure an IPv6 multicast border for a specified IPv6 group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IPv6 multicast border is configured by default.

Syntax

ipv6 multicast boundary *acl-name* [**in** | **out**]

no ipv6 multicast boundary *acl-name* [**in** | **out**]

default ipv6 multicast boundary *acl-name* [**in** | **out**]

Parameter Description

acl-name: ACL name used to define the address range of a multicast group. The value is a case-sensitive string of 1 to 99 characters.

in: Indicates that the multicast border takes effect in the inbound direction of the multicast stream.

out: Indicates that the multicast border takes effect in the outbound direction of the multicast stream.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ACL used in this command is a standard ACL. If an extended ACL is used, the filtering result is inaccurate.

This command can be used to filter MLD and PIM-SMv6 protocol packets relevant to the IPv6 multicast group range. Multicast data streams are not sent or received by this multicast border interface.

Examples

The following example configures an IPv6 multicast border for all IPv6 multicast groups (mul-boun) on the VLAN interface SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list mul-boun
Hostname(config-std-nacl)# permit ipv6 ::/0 ::/0
Hostname(config-std-nacl)# exit
Hostname(config)# interface vlan 1
Hostname(config-if)# ipv6 multicast boundary mul-boun
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 multicast route-limit

Function

Run the **ipv6 multicast route-limit** command to configure the maximum number of entries in an IPv6 multicast routing table.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, a maximum of 4000 entries can be added to an IPv6 multicast routing table.

Syntax

ipv6 multicast route-limit *limit* [*threshold*]

no ipv6 multicast route-limit *limit* [*threshold*]

default ipv6 multicast route-limit *limit* [*threshold*]

Parameter Description

limit: Maximum number of entries in an IPv6 multicast routing table. The value range is from 1 to 64000.

threshold: A threshold that triggers an alarm if the number of IPv6 multicast routes reaches this threshold. The value range is from 1 to 64000, and the default value is **64000**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Due to limitations by hardware resources, routing entries that exceed the range permitted by hardware must be forwarded by software, which causes performance to decrease.

The configured value of *threshold* must be smaller than or equal to the configured value of *limit*.

Examples

The following example sets the maximum number of entries that can be added to an IPv6 multicast routing table to 100 and sets the threshold to 90.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 multicast route-limit 100 90
```

Notifications

When the configured value of threshold is greater than the limit, the following notification will be displayed:

```
Hostname# enable
Hostname# configure terminal
Hostname(config)# ipv6 multicast route-limit 400 4000
% Route threshold exceeds configured route limit
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mroute count**

1.6 ipv6 multicast-routing

Function

Run the **ipv6 multicast-routing** command to enable the IPv6 multicast routing function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The IPv6 multicast routing function is disabled by default.

Syntax

ipv6 multicast-routing

no ipv6 multicast-routing

default ipv6 multicast-routing

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The IPv6 multicast routing function must be enabled prior to different IPv6 multicast protocols.

The IPv6 multicast routing function and the MLD Snooping function are mutually exclusive.

Examples

The following example enables the IPv6 multicast routing function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 multicast-routing
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ipv6 multicast rpf longest-match

Function

Run the **ipv6 multicast rpf longest-match** command to enable the function of RPF route selection based on the longest match rule.

Run the **no** form of this command to select the route with the highest priority as the RPF route.

Run the **default** form of this command to restore the default configuration.

By default, the route with the highest priority is selected as the RPF route. If the routes have the same priority, the RPF route is selected in the order of IPv6 static multicast route, IPv6 MBGP route and IPv6 unicast route.

Syntax

ipv6 multicast rpf longest-match

no ipv6 multicast rpf longest-match

default ipv6 multicast rpf longest-match

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The steps for selecting an RPF route are as follows:

(1) Select one optimal route used for the RPF check from each of the IPv6 static multicast routing table, IPv6 MBGP routing table and IPv6 unicast routing table. Select one route out of the three optimal routes as the RPF route.

(2) If the command for selecting the RPF route based the longest match rule is configured, the route with the longest match is selected out of the three optimal routes as the RPF route. If the three routes share the same subnet mask, the route with the highest priority is selected. If the routes have the same priority, the RPF route is selected in the order of IPv6 static multicast route, IPv6 MBGP route, and IPv6 unicast route.

(3) If the longest match rule is not used, the route with the highest priority is selected as the RPF route. If the routes have the same priority, the RPF route is selected in the order of IPv6 static multicast route, IPv6 MBGP route, and IPv6 unicast route.

Examples

The following example enables the function of RPF route selection based on the longest match rule.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 multicast rpf longest-match
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing**

1.8 ipv6 multicast static

Function

Run the **ipv6 multicast static** command to enable the multicast stream L2 direction control function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

L2 direction control is disabled for multicast streams by default.

Syntax

ipv6 multicast static *ipv6-source-address ipv6-group-address interface-type interface-number*

no ipv6 multicast static *ipv6-source-address ipv6-group-address interface-type interface-number*

default ipv6 multicast static *ipv6-source-address ipv6-group-address interface-type interface-number*

Parameter Description

Ipv6-source -address: Address of a multicast source.

ipv6-group-address: Address of a multicast group.

interface-type interface-number: L2 interface that is allowed to forward the multicast stream.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Multiple commands can be configured for a specified multicast stream so that the stream can be forwarded by multiple interfaces. After direction control is enabled for a multicast stream, this stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream.

This command controls only the forwarding of multicast streams on interfaces, but does not directly affect the processing of multicast protocols on the protocol packets. Some features of multicast protocols (such as PIM-SMv6) are driven by multicast data streams, and therefore, the behavior of the multicast routing protocols may still be affected.

Examples

The following example enables the L2 direction control function for the multicast stream with the source address 2222::3333 and the group address FF66::100, and allows the stream to be forwarded through GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 multicast static 2222::3333 ff66::100 gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 msf6 force-forwarding

Function

Run the **msf6 force-forwarding** command to enable the function of forced forwarding of IPv6 multicast packets (destined for the CPU) by software.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function of forced forwarding of IPv6 multicast packets (destined for the CPU) by software is disabled by default.

Syntax

msf6 force-forwarding

no msf6 force-forwarding

default msf6 force-forwarding

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of forced forwarding of IPv6 multicast packets (destined for the CPU) by software.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# msf6 force-forwarding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 msf6 nsf

Function

Run the **msf6 nsf** command to enable the nonstop forwarding (NSF) function.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The NSF function is not enabled by default.

Syntax

msf6 nsf { **convergence-time** *convergence-time* | **leak** *interval* }

no msf6 nsf { **convergence-time** | **leak** }

default msf6 nsf { **convergence-time** | **leak** }

Parameter Description

convergence-time *convergence-time*: Specifies the maximum convergence time of a multicast protocol, in seconds. The value range is from 0 to 3600, and the default value is **20**.

leak *interval*: Specifies the packet leak time during multicasting, in seconds. The value range is from 0 to 3600, and the default value is **30**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the management board on a device with multiple management boards is switched over, the multicast protocol, for example, PIM-SMv6 or MLD Snooping, takes some time to complete convergence. The NSF parameters are configured to ensure nonstop forwarding of multicast data streams during re-convergence of the multicast protocol.

Examples

The following example enables the NSF function and sets the maximum convergence time of a multicast protocol to 300 seconds and the packet leak time during multicasting to 200 seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname (config)# msf6 nsf convergence-time 300
Hostname (config)# msf6 nsf leak 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show msf6 nsf**

1.11 show ipv6 mroute

Function

Run the **show ipv6 mroute** command to display IPv6 multicast hardware forwarding entries.

Syntax

show ipv6 mroute [*ipv6-group-or-source-address* [*ipv6-group-or-source-address*]]

Parameter Description

ipv6-group-or-source-address: Address of an IPv6 group or source.

ipv6-group-or-source-address: Address of an IPv6 group or source (the two addresses cannot be both group addresses or both source addresses).

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all multicast routing entries.

```
Hostname> enable
Hostname# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
```

```
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SMv6, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

Table 1-1 Output Fields of the show ipv6 mroute Command

Field	Description
Flags	**I**: Collect immediately. **T**: Collect as scheduled. **F**: Set to the hardware forwarding table.
Timers:Uptime/Stat Expiry	The creation time and aging time of this entry.
Interface State	Interface state.
Owner	Owner of this entry, which may be a multicast routing protocol.
Incoming interface	Expected packet inbound interface. If it is inconsistent with the actual inbound interface, the packet is discarded.
Outgoing interface list	Outbound interface list. Packets are forwarded through the interface in the linked list.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show ipv6 mroute count

Function

Run the **show ipv6 mroute count** command to display the count of IPv6 multicast routing entries.

Syntax

show ipv6 mroute count

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the count of IPv6 multicast routing entries.

```
Hostname> enable
Hostname# show ipv6 mroute count
IPv6 Multicast Statistics
Total 1 routes using 168 bytes memory
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 77/147/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0
Immediate/Timed stat updates sent to clients: 0/29
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(2222::1234, ff56::1234), Forwarding: 1/0, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

Table 1-2 Output Fields of the show ipv6 mroute count Command

Field	Description
Total *total-route-number* routes using *memory-size* bytes memory	The total number of routes specified by *total-route-number* occupies *memory-size* bytes.
Route limit/Route threshold	The maximum number of routes/maximum number of configurable routes.
Total NOCACHE/WRONGmif/WHOLEPKT recv from fwd	Number of received unparsed packets/packets through incorrect interfaces/known multicast packets
Total NOCACHE/WRONGmif/WHOLEPKT sent to clients	Number of unparsed packets sent to clients
Immediate/Timed stat updates sent to clients	Number of instantly/scheduled updated packets sent to

Field	Description
	clients
Reg ACK recv/Reg NACK recv/Reg pkt sent	Number of received registration acknowledged packets/received registration unacknowledged packets/sent register packets
Next stats poll	Next status update time
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts	Number of software forwarded packets: Number of packets/Number of bytes Number of other packets: Packets forwarded through incorrect interfaces
Fwd msg counts: WRONGmif/WHOLEPKT recv	Number of forwarded packets: Packets forwarded through incorrect interfaces/Known multicast packets
Client msg counts: WRONGmif/WHOLEPKT/Imm Stat/Timed Stat sent	Number of client packets: Packets forwarded through incorrect interfaces/Known multicast packets/instantly updated packets/scheduled updated packets
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent	Number of registration packets: Received registration acknowledged packets/received registration unacknowledged packets/sent register packets

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show ipv6 mroute sparse

Function

Run the **show ipv6 mroute sparse** command to display PIM-SMv6 multicast core entries.

Syntax

show ipv6 mroute sparse

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SMv6 multicast core entries.

```
Hostname> enable
Hostname# show ipv6 mroute sparse

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
Interface State: Interface
```

Table 1-3 Output Fields of the show ipv6 mroute sparse Command

Field	Description
Flags	**I**- Collect immediately. **T**- Collect as scheduled. **F**- Set to the hardware forwarding table.
Timers:Uptime/Stat Expiry	The creation time and aging time of this entry.
Interface State	Interface state.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show ipv6 mroute static

Function

Run the **show ipv6 mroute static** command to display the IPv6 static multicast routing information.

Syntax

show ipv6 mroute static

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configured static multicast routing information.

```
Hostname> enable
Hostname# show ipv6 mroute static
Mroute: 2233::/64, RPF neighbor: 3333::3333
  Protocol: , distance: 0
```

Table 1-4 Output Fields of the show ipv6 mroute static Command

Field	Description
Mroute	Multicast route.
RPF neighbor	RPF neighbor.
Protocol	Protocol.
distance	Administrative distance.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show ipv6 mroute summary

Function

Run the **show ipv6 mroute summary** command to display the summary information of IPv6 multicast routing entries.

Syntax

show ipv6 mroute summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays summary information of routing entries.

```
Hostname> enable
Hostname# show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

Table 1-5 Output Fields of the show ipv6 mroute summary Command

Field	Description
Flags	**I**- Collect immediately. **T**- Collect as scheduled. **F**- Set to the hardware forwarding table.
Timers:Uptime/Stat Expiry	The creation time and aging time of this entry.
Interface State	Interface state.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show ipv6 mvif

Function

Run the **show ipv6 mvif** command to display IPv6 multicast interface information.

Syntax

show ipv6 mvif [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, all IPv6 multicast interface information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command displays the configured IPv6 multicast interface information that takes effect.

Examples

The following example displays the configured IPv6 multicast interface information that takes effect.

```
Hostname> enable
Hostname# show ipv6 mvif
Interface    Mif   Owner     Uptime
           Idx   Module
Register     0             03d03h09m
VLAN 1       1     PIMSMV6   03d03h09m
```

Table 1-6 Output Fields of the show ipv6 mvif Command

Field	Description
Interface	Interface.

Field	Description
Mif Idx	Index of a multicast interface.
Owner Module	Module name.
Uptime	Start time.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 show ipv6 rpf

Function

Run the **show ipv6 rpf** command to display the RPF information about a specific IPv6 source address.

Syntax

show ipv6 rpf *ipv6-source-address*

Parameter Description

ipv6-source-address: Address of an IPv6 multicast source.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the RPF information about the multicast source 2222::3333.

```
Hostname> enable
Hostname# show ipv6 rpf 2222::3333
  RPF interface: GigabitEthernet 0/1
  RPF neighbor: ::
```

```
RPF route: 2222::/64
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

Table 1-7 Output Fields of the show ipv6 rpf Command

Field	Description
RPF interface	RPF interface.
RPF neighbor	RPF neighbor.
RPF route	RPF route.
RPF type	RPF type.
RPF recursion count	RPF recursion count.
Distance	Administrative distance.
Metric	Metric.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 show ipv6 mrf6 mfc

Function

Run the **show ipv6 mrf6 mfc** command to display IPv6 multicast routing entries.

Syntax

show ipv6 mrf6 mfc [*ipv6-soure-address ipv6-group-address*]

Parameter Description

ipv6-source-address: Source address in an IPv6 multicast routing entry.

ipv6-group-address: Group address in an IPv6 multicast routing entry.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The two parameters are optional, and the source address and group address must be specified simultaneously.

When no source address or group address is specified, all multicast forwarding cache (MFC) entries are displayed.

When the source address and group address are specified, the MFC entries corresponding to the source address and group address are displayed.

Examples

The following example displays the IPv6 L3 multicast hardware forwarding entries with the source address 2001::1.

```
Hostname> enable
Hostname# show ipv6 mrf6 mfc 2001::1 ff06::1
Multicast Routing Forward Cache6 Table
(2001::1, ff06::1)
  FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
  Incoming interface: VLAN 1[4097]
  Outgoing interface list:
VLAN 3 (1)
```

Table 1-8 Output Fields of the show ipv6 mrf6 mfc Command

Field	Description
(*source-address*, *group-address*)	(Source address, group address)
FAST_SW	Flag that indicates whether the entry supports fast forward. If non-Ethernet interface, PPP interface, HDLC interface or frame relay interface exists, no fast forwarded entry is generated.
SWTCHED	Whether an entry is delivered to next-layer hardware forwarding table.
MIN_MTU MTU	Minimum MTU value of an entry.
MIN_MTU_IFINDEX	Index of an interface that has the minimum MTU value.
WRONG IF	Statistics about the multicast data packets from incorrect interfaces.
Incoming interface:*interface-type interface-number*[*lsm-ifx*]	RPF inbound interface of entries. ● *interface-type interface-number*: Interface type and interface number. ● *lsm-ifx*: Index of an LSM interface.
Outgoing interface list:	L3 outbound interface of entries.

Field	Description
interface-type interface-number (*ttl*)	• *interface-type interface-number*: Interface type and interface number. • *ttl*: TTL threshold of this L3 interface.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show msf6 msc

Function

Run the **show msf6 msc** command to display IPv6 L2/L3 multicast hardware forwarding entries.

Syntax

show msf6 msc [*ipv6-soure-address*] [*ipv6-group-address*] [*vlan-id*]

Parameter Description

ipv6-soure-address: IPv6 source address in an L2/L3 multicast hardware forwarding entry.

ipv6-group-address: IPv6 group address in an L2/L3 multicast hardware forwarding entry.

vlan-id: ID of a VLAN to which L2/L3 multicast hardware forwarding entry belongs. When this value is greater than 4096, the interface is a routed port.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

The three parameters are optional.

- When only the source address is specified as S1, all MSC entries corresponding to the source address S1 are displayed.
- When the source address is specified as S1 and the group address is specified as G1, all MSC entries corresponding to the source address S1 and group address G1 are displayed.
- When the source address is specified as S1, the group address is specified as G1, and the VLAN ID is

specified as V1, all MSC entries corresponding to the source address S1, group address G1, and VLAN ID V1 are displayed.

The parameters must be set in order, and a next parameter can be set only when the preceding parameter is set.

If no parameter is specified, all IPv6 L2/L3 multicast hardware forwarding entries are displayed.

Examples

The following example displays the IPv6 L3 multicast hardware forwarding entries with the source address 2012::16:1:0:0:2.

```
Hostname> enable
Hostname# show msf6 msc 2012::16:1:0:0:2
Multicast Switching Cache Table
(2012::16:1:0:0:2, FF1E::2:0:0:1, 4103), HIT, SYNC, MTU:9216, RP_SUP, 2 OIFs
 VLAN 4103(7): 1 OPORTs, FULL, REQ: DONE
   OPORT 7, ROUTER, REQ: DONE
 VLAN 4139(43): 1 OPORTs, FULL, REQ: DONE
   OPORT 43, ROUTER, REQ: DONE
```

Table 1-9 Output Fields of the show msf6 msc Command

Field	Description
(Ipv6-source-address, *ipv6-source-address*, *ipv6-group-address*, *vlan-id*)	(Source address, group address, VLAN ID) Example: (2012::16:1:0:0:2, FF1E::2:0:0:1, 4103)
SYNC	Indicates that the entry is synchronized to the bottom-layer hardware.
MTU	MTU value of an entry.
number OIFs	*Number* of L3 outbound interfaces in an entry
VLAN *vlan-id*(0)	ID of a VLAN to which an L3 outbound interface belongs. When this value is greater than 4096, the interface is a routed port.
oport-number OPORTs	Number of L2 ports that belong to this L3 outbound interface
REQ: DONE	Indicates that this L3 outbound interface has been set to the bottom-layer hardware.
OPORT *oport-index*	Index to the L2 ports that belong to this L3 outbound interface.
MLD-SNP	Indicates that this port is created based on the MLD Snooping protocol. If this value is ROUTER, this port is created based on an L3 protocol.
REQ: DONE	Indicates that this port has been set to the bottom-layer hardware.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show msf6 nsf

Function

Run the **show msf6 nsf** command to display IPv6 multicast NSF configuration.

Syntax

show msf6 nsf

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays multicast NSF configuration.

```
Hostname> enable
Hostname# show msf6 nsf
Multicast HA Parameters
--------+
protocol convergence timeout                   20 secs
flow leak interval                            30 secs
```

Table 1-10 Output Fields of the show msf6 nsf Command

Field	Description

Field	Description
protocol convergence timeout	Maximum period for multicast protocol convergence
flow leak interval	Packet leak time during multicasting

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 MLD Commands

Command	Function
clear ipv6 mld group	Clear dynamic group member records in the MLD cache.
clear ipv6 mld interface	Clear all MLD statistics and group member records on an interface.
ipv6 mld access-group	Specify the address range of multicast groups that an interface can join.
ipv6 mld immediate-leave group-list	Enable the fast leave function on an interface.
ipv6 mld join-group	Add an interface to a group.
ipv6 mld last-member-query-count	Configure the group-specific query packet sending times on an interface.
ipv6 mld last-member-query-interval	Configure the group-specific query packet sending interval on an interface.
ipv6 mld limit	Configure the maximum number of MLD group members.
ipv6 mld mroute-proxy	Enable the MRoute proxy function on an interface.
ipv6 mld proxy-service	Enable the proxy service function on an interface.
ipv6 mld querier-timeout	Configure the other querier keepalive time.
ipv6 mld query-interval	Configure the general group query interval.
ipv6 mld query-max-response-time	Configure the maximum response time of query packets.
ipv6 mld robustness-variable	Configure the robustness variable of the querier.
ipv6 mld ssm-map enable	Enable the SSM mapping function.
ipv6 mld ssm-map static	Configure static mapping entries.
ipv6 mld static-group	Add an interface to a static multicast group.
ipv6 mld version	Configure an MLD version on an interface.
show ipv6 mld groups	Display groups directly connected to the device and group information learned from MLD.
show ipv6 mld interface	Display MLD information about an interface.

show ipv6 mld ssm-mapping	Display SSM mapping information.

1.1 clear ipv6 mld group

Function

Run the **clear ipv6 mld group** command to clear dynamic group member records in the MLD cache.

Syntax

clear ipv6 mld group [*ipv6-group-address*] [*interface-type interface-number*]

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group.

interface-type interface-number: Interface type and interface number of a relevant interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The MLD cache contains a list, which includes multicast groups that hosts in the same directly connected subnet join. If devices join a multicast group, this group is also in the list.

If no parameter is specified, all dynamic group member records are cleared from the MLD cache.

Examples

The following example clears all dynamic group member records.

```
Hostname> enable
Hostname# clear ipv6 mld group
```

The following example clears group member records about the group address FF1E::100.

```
Hostname> enable
Hostname# clear ipv6 mld group ff1e::100
```

The following example clears group member records about the group address FF1E::100 and the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ipv6 mld group ff1e::100 gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear ipv6 mld interface

Function

Run the **clear ipv6 mld interface** command to clear all MLD statistics and group member records on an interface.

Syntax

clear ipv6 mld interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear all group information learned from MLD and packet statistics on an interface. The packet statistics include the number of received report packets, number of done packets, and group member count on the interface.

Examples

The following example clears the MLD statistics and group member records on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ipv6 mld interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ipv6 mld access-group

Function

Run the **ipv6 mld access-group** command to specify the address range of multicast groups that an interface can join.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

An interface can join any group by default.

Syntax

ipv6 mld access-group *acl-name*

no ipv6 mld access-group

default ipv6 mld access-group

Parameter Description

acl-name: ACL name referenced to specify a group address range. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on the interface to specify the address range of multicast groups that hosts in the directly-connected network segment can join. After ACLs are referenced to specify the address range of multicast groups, report packets denied by the ACLs are discarded.

When MLDv2 is enabled, this command supports extended ACLs to precisely filter source record information in MLDv2 reports. If the received MLD report packets follow the format of (S1, S2, S3 … Sn, G), the corresponding ACL is used to check the packets. Therefore, to normally use this command, you must explicitly configure (*, G) in the extended ACLs to filter (S1, S2, S3 … Sn, G).

Examples

The following example configures an ACL on GigabitEthernet 0/1 and sets the source address ranges to ::/64 and 2222::3333/64 and the destination address ranges to FF66::100/64 and FF66::100/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 ::/64 ff66::100/64
Hostname(config-ipv6-acl)# permit ipv6 2222::3333/64 ff66::100/64
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld access-group acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ipv6 mld immediate-leave group-list

Function

Run the **ipv6 mld immediate-leave group-list** command to enable the fast leave function on an interface.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The fast leave function is disabled on an interface by default.

Syntax

ipv6 mld immediate-leave group-list *acl-name*

no ipv6 mld immediate-leave

default ipv6 mld immediate-leave

Parameter Description

acl-name: ACL name referenced to specify a group address range. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This function applies to scenarios where only one user host is connected to an interface.

If this command is not configured, when receiving an MLD leave packet, the interface sends a group-specific query packet and waits for response from the host. If no response is received after timeout, this interface is deleted from the member record. The timeout time refers to the product of the group-specific query interval and robustness variable of MLD. The default value is **2** seconds.

After the fast leave function is enabled, when the device receives a leave packet that specifies a group in the permitted range, the device does not send a group-specific query packet and directly deletes the corresponding group. This reduces the leave latency.

Examples

The following example enables the fast leave function for the groups in the ACL, and sets the source address range in the ACL to 2222::3333/64 and the destination address range to FF66::100/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 2222::3333/64 ff66::100/64
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld immediate-leave group-list acl
```

Notifications

If no ACL is configured for reference, the following notification will be displayed:

```
% access-list acl not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 mld join-group

Function

Run the **ipv6 mld join-group** command to add an interface to a group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface joins any group by default.

Syntax

ipv6 mld join-group *ipv6-group-address*

no ipv6 mld join-group *ipv6-group-address*

default ipv6 mld join-group *ipv6-group-address*

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group. An address starting with 0xFF*1, 0xFF*2, or 0xFF3* is not allowed.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the interface simulates a host and sends a join packet to the uplink devices to join this group.

This command is used for laboratory test.

Examples

The following example adds GigabitEthernet 0/1 to the group FF55::100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld join-group ff55::100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ipv6 mld last-member-query-count

Function

Run the **ipv6 mld last-member-query-count** command to configure the group-specific query packet sending times on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The group-specific query packet sending times is **2** by default.

Syntax

ipv6 mld last-member-query-count *count*

no ipv6 mld last-member-query-count

default ipv6 mld last-member-query-count

Parameter Description

count: Group-specific query packet sending times. The value range is from 2 to 7.

Default Level

14

Command Modes

Interface configuration mode

Usage Guidelines

After receiving a done packet, the interface continuously sends group-specific query packets and waits for responses from hosts. If no response is received after timeout, it is considered that no member exists in the

group in the directly-connected network segment and the interface is deleted from the MLD group member record. The timeout interval is calculated as follows:

Timeout interval = last-member-query-interval × last-member-query-count + query-max-response-time/2

Examples

The following example sets the group-specific query packet sending times to 3 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld last-member-query-count 3
```

Notifications

If the number of group-specific query packet sending times is not within the range from 2 to 7, the following notification will be displayed:

```
% Invalid Last Member Query Count value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.7 ipv6 mld last-member-query-interval

Function

Run the **ipv6 mld last-member-query-interval** command to configure the group-specific query packet sending interval on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The group-specific query packet sending interval is **1** second by default.

Syntax

ipv6 mld last-member-query-interval *interval*

no ipv6 mld last-member-query-interval

default ipv6 mld last-member-query-interval

Parameter Description

interval: Group-specific query packet sending interval, in 0.1 seconds. The value range is from 1 to 255. The default value is 10, indicating 1 second.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After receiving a done packet, the interface continuously sends group-specific query packets and waits for responses from hosts. If no response is received after timeout, it is considered that no member exists in the group in the directly-connected network segment and the interface is deleted from the MLD group member record. The timeout interval is calculated as follows:

Timeout interval = last-member-query-interval × last-member-query-count + query-max-response-time/2

Examples

The following example sets the group-specific query packet sending interval to 2 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld last-member-query-interval 20
```

Notifications

If the value of group-specific query packet sending interval is not within the range from 1 to 255, the following notification will be displayed:

```
% Invalid Last Member Query Interval value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.8 ipv6 mld limit

Function

Run the **ipv6 mld limit** command to configure the maximum number of MLD group members.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the maximum number of MLD group members on an interface is **4000**, and the maximum number of MLD group numbers on a device is **64000**.

Syntax

ipv6 mld limit *limit* [**except** *acl-name*]

no ipv6 mld limit

default ipv6 mld limit

Parameter Description

limit: Maximum number of MLD group members. The value range is from 1 to 64000.

except *access-list*: References an ACL name to specify groups that are not counted. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

In the global configuration mode, the number of members in an MLD group on a device is limited.

In the interface configuration mode, the number of members in an MLD group on an interface is limited.

If the number of group members exceeds the interface limit or global limit, subsequent report packets are ignored.

If an except list is configured, report packets in a specified range can be normally processed, and the records about these group members are not counted.

Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, the global limit prevails.

Examples

The following example sets the maximum number of MLD group members on a device to **400** and sets the maximum number of MLD group members on GigabitEthernet 0/1 to **300**, excluding the groups in the IPv6 list.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list ipv6-list
Hostname(config-ipv6-acl)#permit ipv6 any ff13::/64
Hostname(config)# ipv6 mld limit 400 except ipv6-list
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld limit 300 except ipv6-list
```

Notifications

If the number of MLD group members is not within the range from 1 to 64000, the following notification will be displayed:

```
% Invalid Limit value
```

If the access list is unavailable, the following notification will be displayed:

```
% access-list acl1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.9 ipv6 mld mroute-proxy

Function

Run the **ipv6 mld mroute-proxy** command to enable the MRoute proxy function on an interface.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The MRoute proxy function is disabled by default.

Syntax

ipv6 mld mroute-proxy *interface-type interface-number*

no ipv6 mld mroute-proxy

default ipv6 mld mroute-proxy

Parameter Description

interface-type interface-number: Type and number of an uplink interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The **ipv6 mld proxy-service** command is run to enable the proxy service function on an uplink interface in the root direction of the multicast distribution tree (MDT).

The **ipv6 mld mroute-proxy** command is run to enable the MRoute proxy function on a downlink interface in the leaf direction of the MDT.

The proxy service interface forwards MLD query packets to the MRoute proxy interface. The MRoute proxy interface forwards MLD report packets to the proxy service interface.

Examples

The following example enables the proxy service function on GigabitEthernet 0/1 and the MRoute proxy function on GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld proxy-service
Hostname(config-if-GigabitEthernet 0/1)# exit
```

```
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ipv6 mld mroute-proxy gigabitethernet 0/1
```

Notifications

If the multicast proxy function is already enabled on the current interface, the following notification will be displayed:

```
Mroute proxy had configured
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast route management)
- **show ipv6 mld interface**

1.10 ipv6 mld proxy-service

Function

Run the **ipv6 mld proxy-service** command to enable the proxy service function on an interface.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The proxy service function on an interface is disabled by default.

Syntax

ipv6 mld proxy-service

no ipv6 mld proxy-service

default ipv6 mld proxy-service

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The **ipv6 mld proxy-service** command is run to enable the proxy service function on an uplink interface in the root direction of the MDT.

The **ipv6 mld mroute-proxy** command is run to enable the MRoute proxy function on a downlink interface in the leaf direction of the MDT.

The proxy service interface forwards MLD query packets to the MRoute proxy interface. The MRoute proxy interface forwards MLD report packets to the proxy service interface.

A maximum of 32 proxy service interfaces can be configured on a device. After receiving MLD query packets, the proxy service interface sends report packets based on the MLD group member records.

If the **switchport** command is run on the proxy service interface of a device, the **ipv6 mld mroute-proxy** command configured on the MRoute proxy interface is automatically deleted.

Examples

The following example enables the proxy service function on GigabitEthernet 0/1 and the MRoute proxy function on GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld proxy-service
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ipv6 mld mroute-proxy gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast route management)
- **show ipv6 mld interface**

1.11 ipv6 mld querier-timeout

Function

Run the **ipv6 mld querier-timeout** command to configure the other querier keepalive time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default querier keepalive time is 255 seconds.

Syntax

ipv6 mld querier-timeout *timeout*

no ipv6 mld querier-timeout

default ipv6 mld querier-timeout

Parameter Description

timeout: Other querier keepalive time, in seconds. The value range is from 60 to 300.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When a non-querier does not receive a query packet in the same network segment within a specified period, the non-querier considers there is only one device (itself) in the directly connected network segment and initiates a new round of querier election.

Examples

The following example sets the other querier keepalive time to 200 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld querier-timeout 200
```

Notifications

If the configured other querier keepalive time is not within the range from 60 to 300, the following notification will be displayed:

```
% Invalid Querier Timeout Time value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.12 ipv6 mld query-interval

Function

Run the **ipv6 mld query-interval** command to configure the general group query interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default general group query interval is 125 seconds.

Syntax

ipv6 mld query-interval *interval*

no ipv6 mld query-interval

default ipv6 mld query-interval

Parameter Description

interval: General group query interval, in seconds. The value range is from 1 to 18000.

Default Level

14

Command Modes

Interface configuration mode

Usage Guidelines

N/A

Examples

The following example sets the general group query interval to 120 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld query-interval 120
```

Notifications

If the configured general group query interval is not within the range from 1 to 18000, the following notification will be displayed:

```
% Invalid Query Interval value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.13 ipv6 mld query-max-response-time

Function

Run the **ipv6 mld query-max-response-time** command to configure the maximum response time of query packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum response time of query packets is **10** seconds by default.

Syntax

ipv6 mld query-max-response-time *max-response-time*

no ipv6 mld query-max-response-time

default ipv6 mld query-max-response-time

Parameter Description

max-response-time: Maximum response time of query packets, in seconds. The value range is from 1 to 25.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

A query packet is sent through an interface. If no response is received after timeout, it is considered that no member exists in the group of the directly connected network segment and the group information is deleted.

Examples

The following example sets the maximum response time of query packets to 20 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld query-max-response-time 20
```

Notifications

If the configured maximum response time of query packets is not within the range from 1 to 240, the following notification will be displayed:

```
% Invalid Query Max-Response Time value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.14 ipv6 mld robustness-variable

Function

Run the **ipv6 mld robustness-variable** command to configure the robustness variable of the querier.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The querier robustness variable is **2** by default.

Syntax

ipv6 mld robustness-variable *robustness*

no ipv6 mld robustness-variable

default ipv6 mld robustness-variable

Parameter Description

robustness: Robustness variable of the querier. The value range is from 2 to 7.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the robustness variable of the querier to 3 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld robustness-variable 3
```

Notifications

If the configured robustness variable of the querier is not within the range from 2 to 7, the following notification will be displayed:

```
% Invalid Robustness Variable value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.15 ipv6 mld ssm-map enable

Function

Run the **ipv6 mld ssm-map enable** command to enable the SSM mapping function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SSM mapping function is disabled by default.

Syntax

ipv6 mld ssm-map enable

no ipv6 mld ssm-map enable

default ipv6 mld ssm-map enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **ipv6 mld ssm-map static** command is run to configure static mapping entries.

The interface runs MLDv2. When receiving MLDv1 report packets, a multicast device adds the static mapping source address.

Examples

The following example enables the SSM mapping function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld ssm-map enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim ssm** (PIM-SMv6)
- **ipv6 mld ssm-map static**
- **show ipv6 mld ssm-mapping**

1.16 ipv6 mld ssm-map static

Function

Run the **ipv6 mld ssm-map static** command to configure static mapping entries.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static mapping entry is configured by default.

Syntax

ipv6 mld ssm-map static *acl-name ipv6-source-address*

no ipv6 mld ssm-map static *acl-name ipv6-source-address*

default ipv6 mld ssm-map static *acl-name ipv6-source-address*

Parameter Description

acl-name: ACL name referenced to specify a group address range. The value is a case-sensitive string of 1 to 99 characters.

ipv6-source-address: Address of an IPv6 multicast source.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The **ipv6 mld ssm-map enable** command is run to enable the SSM mapping function.

The interface runs MLDv2. When receiving MLDv1 report packets, a multicast device adds the static mapping source address.

Examples

The following example enables the SSM mapping function, and sets the group address of static mapping entries to ACL ASD and the source address to 4444::1234.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list asd
Hostname(config-ipv6-acl)# permit ipv6 any FF34::/64
Hostname(config)# ipv6 mld ssm-map enable
Hostname(config)# ipv6 mld ssm-map static asd 4444::1234
```

Notifications

If *ipv6-source-address* is not a multicast address, the following notification will be displayed:

```
% Invalid input, not a unicast IP address 4444::1234!
```

If the name of the access list does not comply with specifications, the following notification will be displayed:

```
% Invalid access list name
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim ssm** (PIM-SMv6)
- **ipv6 mld ssm-map enable**
- **show ipv6 mld ssm-mapping**

1.17 ipv6 mld static-group

Function

Run the **ipv6 mld static-group** command to add an interface to a static multicast group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is added to any static multicast group by default.

Syntax

ipv6 mld static-group *ipv6-group-address*

no ipv6 mld static-group *ipv6-group-address*

default ipv6 mld static-group *ipv6-group-address*

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, an interface can join a group without MLD packet interaction. Even if no host in the same directly connected network segment as this interface joins this group, this interface is in the member record of this group.

The member record that is generated by adding an interface to a static group cannot be deleted by running the **clear ipv6 mld group** command, and can be deleted by running the **no ipv6 mld static-group** command.

Examples

The following example adds GigabitEthernet 0/1 to the group FF55::3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld static-group ff55::3
```

Notifications

If an interface fails to join a static group, the following notification will be displayed:

```
Static-group create fail! addr= ff55::3
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.18 ipv6 mld version

Function

Run the **ipv6 mld version** command to configure an MLD version on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

MLDv2 is running on an interface by default.

Syntax

ipv6 mld version { **1** | **2** }

no ipv6 mld version

default ipv6 mld version

Parameter Description

1: Uses MLDv1.

2: Uses MLDv2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the MLD process automatically restarts.

A device is backward compatible, and can process MLD packets of the same version or earlier version. It is recommended that the MLD version of the device be later than or equal to that of a host.

Examples

The following example configures MLDv1 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld version 1
```

Notifications

If the version number is not within the range from 1 to 3, the following notification will be displayed:

```
% Invalid Version value:
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld interface**

1.19 show ipv6 mld groups

Function

Run the **show ipv6 mld groups** command to display groups directly connected to the device and group information learned from MLD.

Syntax

show ipv6 mld groups [*ipv6-group-address* | *interface-type interface-number*] [**detail**]

Parameter Description

ipv6-group-address: Address of a specified IPv6 multicast group.

interface-type interface-number: Type and number of a specified interface.

detail: Displays detailed information about an IPv6 multicast group. If this parameter is not specified, the summary information about the multicast group is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified, the summary information about all multicast groups learned from all interfaces is displayed.

Examples

The following example displays all group information.

```
Hostname> enable
Hostname# show ipv6 mld groups
MLD Connected Group Membership
Group Address   Interface   Uptime     Expires    Last Reporter
ff66::1         VLAN1       00:10:57   00:02:16   fe80::2d0:f8ff:fe22:3378
```

The following example displays detailed information about a group.

```
Hostname> enable
Hostname# show ipv6 mld groups detail
Interface:     VLAN 1
Group:         ff66::1
Uptime:        00:10:26
Group mode:    Exclude (Expires: 00:02:47)
Last reporter:  fe80::2d0:f8ff:fe22:3378
Source list is empty
```

Table 1-1 Output Fields of the show ipv6 mld groups Command

Field	Description
Group Address	Group address.
Interface	Interface.
Uptime	Update time.
Group mode	Group record filtering mode. The values of this field are as follows: ● Include ● Exclude
Expires	Entry timeout time.
Last Reporter	Address of the last member that sends report packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ipv6 mld interface

Function

Run the **show ipv6 mld interface** command to display MLD information about an interface.

Syntax

show ipv6 mld interface [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the MLD information about all interfaces is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays MLD information about all interfaces.

```
Hostname> enable
Hostname# show ipv6 mld interface
Interface VLAN 2 (Index 4098)
 MLD Enabled, Inactive, Version 2 (default)
 MLD interface limit is 1024
 MLD interface has 0 group-record states
 MLD interface has 1 join-group records
 MLD interface has 0 static-group records
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 10 (1/10s)
 Last member query count is 2
 Group Membership interval is 260
 Robustness Variable is 2
```

Table 1-2 Output Fields of the show ipv6 mld interface Command

Field	Description
Interface	Interface.

Field	Description
MLD interface limit is x	Maximum number of group members on an MLD interface.
MLD interface has x group-record states	Number of group record states on an interface.
MLD interface has x join-group records	Number of member join records on an interface.
MLD interface has x static-group records	Number of static group records on an interface.
MLD query interval is x seconds	MLD query interval, in seconds.
MLD querier timeout is x seconds	MLD query timeout time, in seconds.
MLD max query response time is x seconds	Maximum response time of MLD query, in seconds.
Last member query response interval is *last-member-query-response-interval* (1/10s)	Last member query interval, in 0.1 seconds.
Last member query count is *last-member-query-count*	Last member query times.
Group Membership interval is *group-membership-interval*	Membership sending interval.
Robustness Variable is *robustness*	Robustness variable.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show ipv6 mld ssm-mapping

Function

Run the **show ipv6 mld ssm-mapping** command to display SSM mapping information.

Syntax

show ipv6 mld ssm-mapping [*ipv6-group-address*]

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group. If this parameter is not specified, all MLD SSM mapping information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the SSM mapping information of the group FF66::1234.

```
Hostname> enable
Hostname# show ipv6 mld ssm-mapping ff66::1234
Group address: ff66::1234
Database    : Static
Source list  : 5555::1234
```

Table 1-3 Output Fields of the show ipv6 mld ssm-mapping Command

Field	Description
Group Address	Group address.
Database	Data state.
Source list	Linked list of source addresses.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 PIM-SMv6 Commands

Command	Function
clear ipv6 mroute	Clear IPv6 multicast routing entries.
clear ipv6 mroute statistics	Clear statistics about IPv6 multicast routing entries.
clear ipv6 pim sparse-mode bsr rp-set	Clear all dynamic rendezvous point (RP) information.
clear ipv6 pim sparse-mode track	Set the statistics start time and clear statistics of the PIMv6 packets.
ipv6 pim accept-bsr list	Limit the address range of BSRs.
ipv6 pim accept-crp-with-null-group	Enable the BSR to receive advertisement packets with the prefix of a multicast address being 0.
ipv6 pim accept-crp list	Limit the C-RP address range and the address range of the groups served by the C-RPs.
ipv6 pim accept-register	Limit the (S, G) address range in the register messages received by an RP.
Ipv6 pim bsr-border	Configure a BSR border.
ipv6 pim bsr-candidate	Configure C-BSRs.
ipv6 pim bfd	Configure the BFD Support for PIMv6 feature on an interface, also known as PIMv6 BFD.
ipv6 pim dr-priority	Configure the DR priority.
Ipv6 pim ignore-rp-set-priority	Ignore RP priority for RP election.
ipv6 pim jp-timer	Configure the join/prune packet sending interval.
ipv6 pim neighbor-filter	Enable the neighbor filtering function.
ipv6 pim neighbor-tracking	Enable the neighbor tracking function.
ipv6 pim override-interval	Configure the prune override interval of an interface.
ipv6 pim probe-interval	Configure the register-probe time.
ipv6 pim propagation-delay	Configure the propagation delay of an interface.
ipv6 pim query-interval	Configure the hello message sending interval.
ipv6 pim register-checksum-wholepkt	Calculate the checksum of entire register messages.
ipv6 pim register-rate-limit	Limit the sending rate of register messages.

ipv6 pim register-rp-reachability	Enable the RP reachability checking function before a register message is sent.
ipv6 pim register-source	Specify a source IPv6 address in register messages.
ipv6 pim register-suppression	Configure the register suppression time.
ipv6 pim rp-address	Configure static RPs.
ipv6 pim rp-candidate	Configure C-RPs.
ipv6 pim rp-register-kat	Configure the (S, G) entry timeout period on an RP.
ipv6 pim rp embedded	Enable the RP address embedding function.
ipv6 pim sparse-mode	Enable the PIM-SMv6 function on an interface.
ipv6 pim sparse-mode passive	Enable the PIM-SMv6 passive mode on an interface.
ipv6 pim spt-threshold	Enable the shortest path tree (SPT) switchover function.
ipv6 pim ssm	Enable the SSM function and configure an SSM group address range.
ipv6 pim static-rp-preferred	Configure static DR priority to be higher than dynamic RP priority.
ipv6 pim triggered-hello-delay	Configure the hello message sending delay on an interface.
show ipv6 pim sparse-mode bsr-router	Display BSR information.
show ipv6 pim sparse-mode interface	Display PIM-SMv6 information of an interface.
show ipv6 pim sparse-mode local-members	Display local MLD information of a PIM-SMv6 interface.
show ipv6 pim sparse-mode mroute	Display PIM-SMv6 routing information.
show ipv6 pim sparse-mode neighbor	Display neighbor information.
show ipv6 pim sparse-mode nexthop	Display next hop information, including interface, address, and metric value of a next hop.
show ipv6 pim sparse-mode rp mapping	Display all RPs and the groups served by the RPs on the local device.
show ipv6 pim sparse-mode rp-hash	Display RP information corresponding to a multicast group address.
show ipv6 pim sparse-mode track	Display the number of PIM packets sent and received since the statistic start time.

1.1 clear ipv6 mroute

Function

Run the **clear ipv6 mroute** command to clear IPv6 multicast routing entries.

Syntax

clear ipv6 mroute { ***** | *ipv6-group-address* [*ipv6-source-address*] }

Parameter Description

*****: Clears all IPv6 multicast routing entries.

ipv6-group-address: Address of an IPv6 multicast group whose routing entries are to be cleared.

ipv6-source-address: Address of an IPv6 multicast source whose routing entries are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the multicast function fails, you can run this command to clear the current multicast routing information to facilitate problem locating and re-learn entries.

Examples

The following example clears all IPv6 multicast routing entries.

```
Hostname> enable
Hostname# clear ipv6 mroute *
```

The following example clears IPv6 multicast routing entries of a specified group.

```
Hostname> enable
Hostname# clear ipv6 mroute ff66::6666
```

The following example clears multicast routing entries of a specified group and source.

```
Hostname> enable
Hostname# clear ipv6 mroute ff66::6666 3333::3333
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 mroute statistics

Function

Run the **clear ipv6 mroute statistics** command to clear statistics about IPv6 multicast routing entries.

Syntax

clear ipv6 mroute statistics { ***** | *ipv6-group-address* [*ipv6-source-address*] }

Parameter Description

*****: Clears all statistics about multicast routing entries.

ipv6-group-address: Address of a specified IPv6 multicast group whose routing entry statistics are to be cleared.

ipv6-source-address: Address of a specified IPv6 multicast source whose routing entry statistics are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the multicast function fails, you can run this command to clear the current multicast routing statistics to facilitate problem locating and re-collect information.

Examples

The following example clears statistics about all multicast routing entries.

```
Hostname> enable
Hostname# clear ipv6 mroute statistics *
```

The following example clears statistics about multicast routing entries of a specified group.

```
Hostname> enable
Hostname# clear ipv6 mroute statistics ff66::6666
```

The following example clears statistics about multicast routing entries of a specified group and source.

```
Hostname> enable
Hostname# clear ipv6 mroute statistics ff66::6666 3333::3333
```

Notifications

N/A

Platform Description

N/A

1.3 clear ipv6 pim sparse-mode bsr rp-set

Function

Run the **clear ipv6 pim sparse-mode bsr rp-set** command to clear all dynamic rendezvous point (RP) information.

Syntax

clear ipv6 pim sparse-mode bsr rp-set *

Parameter Description

*****: Clears all dynamic RP information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear dynamic C-RP information, rather than static C-RP information.

Examples

The following example clears all dynamic RP information of PIM-SMv6.

```
Hostname> enable
Hostname# clear ipv6 pim sparse-mode bsr rp-set *
```

Notifications

After the RP-Set information is cleared, the following notification will be displayed:

```
Self RP is changed for group range %R/%u.  Perform Self RP change handler
```

Platform Description

N/A

1.4 clear ipv6 pim sparse-mode track

Function

Run the **clear ipv6 pim sparse-mode track** command to set the statistics start time and clear statistics of the PIMv6 packets.

Syntax

clear ipv6 pim sparse-mode track

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example resets the statistic start time and clears statistics of the PIMv6 packets.

```
Hostname> enable
Hostname# clear ipv6 pim sparse-mode track
```

Notifications

N/A

Platform Description

N/A

1.5 ipv6 pim accept-bsr list

Function

Run the **ipv6 pim accept-bsr list** command to limit the address range of BSRs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All BSMs are received by default.

Syntax

ipv6 pim accept-bsr list *acl-name*

no ipv6 pim accept-bsr

default ipv6 pim accept-bsr

Parameter Description

list *acl-name*: Uses an ACL name to limit the address range of BSRs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example uses the ACL bsr-list to limit the address range of BSRs so that only BSMs sent from the BSRs in the bsr-list range are received.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list bsr-list
Hostname(config-ipv6-acl)# permit ipv6 9000::5/64 any
```

```
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-bsr list bsr-list
```

Notifications

If no ACL is configured to limit the BSR address range, the following notification will be displayed:

```
% access-list bsr-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim bsr-candidate**

1.6 ipv6 pim accept-crp-with-null-group

Function

Run the **ipv6 pim accept-crp-with-null-group** command to enable the BSR to receive advertisement packets with the prefix of a multicast address being 0.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function for the BSR to receive advertisement packets with the prefix of a multicast address being 0 is disabled by default.

Syntax

ipv6 pim accept-crp-with-null-group

no ipv6 pim accept-crp-with-null-group

default ipv6 pim accept-crp-with-null-group

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A C-RP periodically sends advertisement packets to the BSR in unicast mode. The packets include the RP priority, advertisement packet hold time (greater than the interval of sending the advertisement packet), RP address, address of the served group, and prefix of the multicast address. Upon receiving the advertisement

packets, the BSR collects the information in the packets as RP-Set in the advertisement packet hold time, encapsulates the information in a BSM, and sends the message to all PIM devices.

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can receive advertisement packets with the prefix of a multicast address being 0. This C-RP can serve all groups.

Examples

The following example configures the BSR to receive advertisement packets with the prefix of the multicast address being 0 from a C-RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim accept-crp-with-null-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ipv6 pim accept-crp list

Function

Run the **ipv6 pim accept-crp list** command to limit the C-RP address range and the address range of the groups served by the C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The C-BSRs receive all external C-RP advertisement packets by default.

Syntax

ipv6 pim accept-crp list *acl-name*

no ipv6 pim accept-crp

default ipv6 pim accept-crp

Parameter Description

list *acl-name*: Uses an ACL name to limit the C-RP address range and the address range of the groups served by the C-RPs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can limit the C-RP address range and the address range of the groups served by the C-RPs.

Examples

The following example uses the ACL crp-list to limit the C-RP address range and the address range of the groups served by the C-RPs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list crp-list
Hostname(config-ipv6-acl)# permit ipv6 9000::5/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-crp list crp-list
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list crp-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim rp-candidate**

1.8 ipv6 pim accept-register

Function

Run the **ipv6 pim accept-register** command to limit the (S, G) address range in the register messages received by an RP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The (S, G) address range of register messages is not limited by default. An RP receives register messages with any (S, G) address.

Syntax

ipv6 pim accept-register { **list** *acl-name* | **route-map** *route-map-name* } *

no ipv6 pim accept-register

default ipv6 pim accept-register

Parameter Description

list *acl-name*: Uses an ACL name to limit the (S, G) group address range. The value is a case-sensitive string of 1 to 99 characters.

route-map *route-map-name*: Uses a route map to limit the (S, G) address range.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a static RP or C-RP, the RP replies a register-stop message upon receiving data from an unauthorized source.

Examples

The following example uses an ACL register-access-list to deny register messages from the source FE80::2D0:F8FF:FE22:33AD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list register-access-list
Hostname(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-register list register-access-list
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 Ipv6 pim bsr-border

Function

Run the **ipv6 pim bsr-border** command to configure a BSR border.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BSR border is configured by default.

Syntax

ipv6 pim bsr-border
no ipv6 pim bsr-border
default ipv6 pim bsr-border

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To control BSM flooding, you can configure a BSR border on the interface. Then, this interface discards received BSMs without forwarding them.

Examples

The following example configures a BSR border on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim bsr-border
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast boundary** (IPv6 multicast route management)
- **show ipv6 pim sparse-mode interface**

1.10 ipv6 pim bsr-candidate

Function

Run the **ipv6 pim bsr-candidate** command to configure C-BSRs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No C-BSR is configured by default.

Syntax

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ipv6 pim bsr-candidate

Parameter Description

interface-type terface-number: Interface type and interface number. You are advised to use the address of this interface as the address of a C-BSR.

hash-mask-length: Length of a hash mask configured for the RP election mechanism. The value range is from 0 to 128, and the default value is **126**.

priority-value: C-BSR priority. The value range is from 0 to 255, and the default value is **64**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In a PIM SMv6 domain, a unique BSR must be available. The BSR collects and releases RP information. Multiple C-BSRs elect an acknowledged BSR based on BSMs. Before a BSR is elected, each C-BSR considers itself a BSR and periodically sends a BSM in the PIM-SMv6 domain. This message includes the address and priority of the BSR.

This command can be used to send a BSM to all PIM neighbors through the address assigned to a BSR. Each neighbor compares the original BSR address with the address in the received BSM. If the received BSM indicates that the C-BSR of the received BSM boasts a higher priority or a larger IP address, the neighbor saves the address in the BSM as the BSR address and forwards the BSM. Otherwise, the neighbor discards the BSM.

A C-BSR considers itself the BSR until the C-BSR receives a BSM indicating a higher priority from another C-BSR.

Examples

The following example configures the address of GigabitEthernet 0/1 as the address of a C-BSR, and sets the length of the hash mask to 30 and the priority to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim bsr-candidate gigabitethernet 0/1 30 100
```

Notifications

If the current interface is not configured in SM mode, the following notification will be displayed:

```
Warning: PIMSMv6 not configured on %s, BSR messages not originated.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 pim bfd

Function

Run the **ipv6 pim bfd** command to configure the BFD Support for PIMv6 feature on an interface, also known as PIMv6 BFD.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

PIMv6 BFD is not configured on an interface by default.

Syntax

ipv6 pim bfd

no ipv6 pim bfd

default ipv6 pim bfd

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Bidirectional forwarding detection (BFD) is used to quickly detect or monitor links or IP route forwarding connectivity in a network.

Based on the PIM-SMv6 protocol, a designated router (DR) is defined. This DR is the unique role that forwards multicast data in a shared network.

Devices in the shared network exchange PIM hello messages and elect a DR based on the hello messages. When the DR is faulty, a new round of DR election can be started only after the PIM neighbor ages. If this command is run, when the DR is faulty, this faulty DR can be detected and a new round of election can be started in milliseconds.

Examples

The following example configures PIMv6 BFD on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname (config-if-GigabitEthernet 0/1)# ipv6 pim bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim sparse-mode**
- **show bfd neighbors** (reliability/BFD)

1.12 ipv6 pim dr-priority

Function

Run the **ipv6 pim dr-priority** command to configure the DR priority.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default DR priority is **1**.

Syntax

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

default ipv6 pim dr-priority

Parameter Description

priority-value: DR priority. A larger value indicates a higher priority. The value range is from 0 to 4294967294.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If multiple devices in a LAN join DR election, the election result is subject to the priorities in hello messages. The device with the highest priority is elected as the DR. If the priorities in the hello messages are the same or the priority parameter is not set in the hello messages, the device with the largest IP address is elected as the DR.

Examples

The following example sets the DR priority to **11234** on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim dr-priority 11234
```

Notifications

If the priority value is smaller than 0, the following notification will be displayed:

```
% Invalid DR priority value.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.13 Ipv6 pim ignore-rp-set-priority

Function

Run the **ipv6 pim ignore-rp-set-priority** command to ignore RP priority for RP election.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A C-RP with the highest priority is selected as the RP by default.

Syntax

Ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

default ipv6 pim ignore-rp-set-priority

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example ignores RP priority for RP election.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim ignore-rp-set-priority
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 pim jp-timer

Function

Run the **ipv6 pim jp-timer** command to configure the join/prune packet sending interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The join/prune packet is sent at an interval of **60** seconds by default.

Syntax

ipv6 pim jp-timer *interval*

no ipv6 pim jp-timer

default ipv6 pim jp-timer

Parameter Description

interval: Join/prune packet sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the join/prune packet sending interval to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 pim jp-timer 100
```

Notifications

If the join/prune packet sending interval is not within the range from 0 to 65535, the following notification will be displayed:

```
% Invalid Join/Prune timer value.
```

If the value of *interval* is greater than the maximum time of adding a prune packet, the following notification will be displayed:

```
WARNING: PIMv2 J/P timer too high, changed %u to %u sec
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ipv6 pim neighbor-filter

Function

Run the **ipv6 pim neighbor-filter** command to enable the neighbor filtering function.

Run **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor filtering function is disabled by default.

Syntax

ipv6 pim neighbor-filter *acl-name*

no ipv6 pim neighbor-filter *acl-name*

default ipv6 pim neighbor-filter *acl-name*

Parameter Description

acl-name: ACL name that is used to limit the address range of neighbors. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The neighbor filtering function can strengthen PIM network security and limit the valid address range of neighbors. If a neighbor is filtered out based on an access filtering list, PIM-SMv6 does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

Examples

The following example uses the ACL to deny requests for establishing peer relationship with the neighbor FE80::2D0:F8FF:FE22:33AD on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim neighbor-filter acl
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list acl not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.16 ipv6 pim neighbor-tracking

Function

Run the **ipv6 pim neighbor-tracking** command to enable the neighbor tracking function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor tracking function is disabled by default.

Syntax

Ipv6 pim neighbor-tracking

no ipv6 pim neighbor-tracking

default ipv6 pim neighbor-tracking

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the suppression capability of an interface is enabled, when the local router plans to send a join packet to an uplink neighbor but it receives a join packet sent from the neighbor to the uplink router, this local router suppresses its own join packet. If the suppression capability of the interface is disabled, the join packet can be sent. When the suppression capability of downlink hosts is disabled, an uplink device can determine the number of the downlink hosts based on the quantity of received join packets. This is neighbor tracking.

Examples

The following example disables the suppression function on GigabitEthernet 0/1 and enables neighbor tracking.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim neighbor-tracking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ipv6 pim override-interval

Function

Run the **ipv6 pim override-interval** command to configure the prune override interval of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default prune override interval of an interface is **2500** ms.

Syntax

ipv6 pim override-interval *override-interval*

no ipv6 pim override-interval

default ipv6 pim override-interval

Parameter Description

override-interval: Prune override interval of an interface, in milliseconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or prune override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the join/prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the prune override interval to 3000 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim override-interval 3000
```

Notifications

If the configured prune override interval is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid Hello option: override-interval value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim propagation-delay**
- **show ipv6 pim sparse-mode interface**

1.18 ipv6 pim probe-interval

Function

Run the **ipv6 pim probe-interval** command to configure the register-probe time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default register-probe time is **5** seconds.

Syntax

ipv6 pim probe-interval *interval*

no ipv6 pim probe-interval

default ipv6 pim probe-interval

Parameter Description

interval: Register-probe interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The register-probe time refers to the time when the source DR is allowed to send null register messages to the RP before the register suppression timer times out.

The register-probe time cannot be greater than a half of the register suppression time. Otherwise, the configuration fails and an alarm is generated.

The sum of the three times of register suppression time and the register-probe time does not exceed 65535. Otherwise, the configuration fails and an alarm is generated.

Examples

The following example sets the register-probe time to 6 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim probe-interval 6
```

Notifications

If the configured register-probe time is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid probe-interval value
```

If two times of the register-probe time is greater than the register suppression time, the following notification will be displayed:

```
WARNING: Register probe interval MUST be less than half the register suppression
interval. Please set a less one.
```

If the sum of three times of register suppression time and the register-probe time is greater than 65535, the following notification will be displayed:

```
WARNING: Register probe interval is too large. It may cause (3*RST+probe-
interval) > 65535.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ipv6 pim propagation-delay

Function

Run the **ipv6 pim propagation-delay** command to configure the propagation delay of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default propagation delay of an interface is **500** ms.

Syntax

ipv6 pim propagation-delay *propagation-delay*

no ipv6 pim propagation-delay

default ipv6 pim propagation-delay

Parameter Description

propagation-delay: Propagation delay of an interface, in milliseconds. The value range is from 1 to 32767.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or prune override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the join/prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the prune override delay to 600 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim propagation-delay 600
```

Notifications

If the configured prune override delay is not within the range from 1 to 32767, the following notification will be displayed:

```
% Invalid Hello option: propagation-delay value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim override-interval**
- **show ipv6 pim sparse-mode interface**

1.20 ipv6 pim query-interval

Function

Run the **ipv6 pim query-interval** command to configure the hello message sending interval.

Run the **no** form of command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The hello message is sent at an interval of **30** seconds by default.

Syntax

ipv6 pim query-interval *interval*

no ipv6 pim query-interval

default ipv6 pim query-interval

Parameter Description

interval: Hello message sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the hello message sending interval is updated, the hello message hold time is updated accordingly. The hello message hold time is 3.5 times of the hello message sending interval. If the product of the hello message sending interval and 3.5 is greater than 65535, the hello message sending interval is forcibly reset to 18725.

Examples

The following example sets the hello message sending interval to 60 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim query-interval 60
```

Notifications

If the configured hello message sending interval is not within the range from 1 to 32767, the following notification will be displayed:

```
% Invalid Query interval value
```

If the value of *interval* is greater than the maximum time of a request interval, the following notification will be displayed:

```
WARNING: PIMv2 Query interval too high, changed %u to %d sec.
(corresponding to maximum holdtime 0xFFFF)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.21 ipv6 pim register-checksum-wholepkt

Function

Run the **ipv6 pim register-checksum-wholepkt** command to calculate the checksum of entire register messages.

Run the **no** form of this command to remove this configuration and calculate the checksum of headers of PIM packets and register messages, rather than the entire packets.

Run the **default** form of this command to restore the default configuration.

By default, only the headers of PIM packets and register messages, rather than the entire packets, are specified for calculating the checksum.

Syntax

ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

no ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

default ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups that support this configuration. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The checksum of the entire PIM protocol packets (including encapsulated multicast packets), rather than the PIM headers of separate register messages, is calculated.

If the **group-list** parameter is not specified, the entire packet checksum calculation method applies to register messages with any group address.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits of the ACL associated with the **group-list** parameter are removed. In this case, the entire packet checksum calculation method applies to register messages with any group address.

Examples

The following example uses the ACL checksum-access-list to apply the entire packet checksum calculation method to the register messages with the multicast group address FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list checksum-access-list
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim register-checksum-wholepkt group-list checksum-access-
list
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list checksum-access-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ipv6 pim register-rate-limit

Function

Run the **ipv6 pim register-rate-limit** command to limit the sending rate of register messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The sending rate of register messages is not limited by default.

Syntax

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

default ipv6 pim register-rate-limit

Parameter Description

rate: Maximum number of register messages that can be sent per second. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the sending rate of register messages in (S, G) status, rather than that of the entire system. Running this command can reduce the load of the source DR and RP. Register messages sent at a rate exceeding the limit are discarded.

Examples

The following example limits the sending rate of register messages to 3000 per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-rate-limit 3000
```

Notifications

If the configured sending rate of register messages is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid Limit value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ipv6 pim register-rp-reachability

Function

Run the **ipv6 pim register-rp-reachability** command to enable the RP reachability checking function before a register message is sent.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The RP reachability checking function before a register message is sent is disabled by default.

Syntax

ipv6 pim register-rp-reachability

no ipv6 pim register-rp-reachability

default ipv6 pim register-rp-reachability

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the RP reachability is checked before a register message is sent. If the RP is reachable, the register message is sent. Otherwise, the register message is not sent.

Examples

The following example enables the RP reachability checking function before a register message is sent.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-rp-reachability
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ipv6 pim register-source

Function

Run the **ipv6 pim register-source** command to specify a source IPv6 address in register messages.

Run the **no** form of this command to remove this configuration and use the address of the DR interface connected to the source as the source IPv6 address in register messages.

Run the **default** form of this command to restore the default configuration.

The source IPv6 address in register messages is the address of the DR interface connected to the source by default.

Syntax

ipv6 pim register-source { *ipv6-local-address* | *interface-type interface-number* }

no ipv6 pim register-source

default ipv6 pim register-source

Parameter Description

ipv6-local-address: Source IPv6 address in register messages.

interface-type interface-number: Interface type and interface number. The IPv6 address of this interface is specified as the source address in register messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the RP reachability is checked before a register message is sent. If the RP is reachable, the message is sent. Otherwise, the message is not sent.

It is recommended that loopback address be used as the source IP address in register messages. Other physical addresses can be used as the source IP addresses in register messages as well.

Examples

The following example specifies the IPv6 address 3333::3333 as the source address in register messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-source 3333::3333
```

The following example specifies the IPv6 address of GigabitEthernet 0/1 as the source IP address in register messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-source gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ipv6 pim register-suppression

Function

Run the **ipv6 pim register-suppression** command to configure the register suppression time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default register suppression time is **60** seconds.

Syntax

ipv6 pim register-suppression *suppression-time*

no ipv6 pim register-suppression

default ipv6 pim register-suppression

Parameter Description

suppression-time: Register suppression time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be run on the DR to configure the register message suppression time.

If the **ipv6 pim rp-register-kat** command is not run, configuring the register suppression time on the RP changes the (S, G) entry timeout period. The (S, G) entry timeout period on an RP is the sum of three times of the register suppression time and the register-probe time.

Examples

The following example sets the register suppression time to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-suppression 100
```

Notifications

If the configured register suppression time is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid KAT value
```

If two times of the register-probe time is greater than the register message suppression time, the following notification will be displayed:

```
WARNING: Register suppression interval MUST be larger than twice the register
probe interval. Please set a larger one.
```

If the sum of three times of register suppression time and the register-probe time is greater than 65535, the following notification will be displayed:

```
WARNING: Register suppression interval is too large. It may cause (3*RST+probe-interval) > 65535.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ipv6 pim rp-address

Function

Run the **ipv6 pim rp-address** command to configure static RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static RP is configured by default.

Syntax

ipv6 pim rp-address *ipv6-rp-address* [*acl-name*]

no ipv6 pim rp-address *ipv6-rp-address*

default ipv6 pim rp-address *ipv6-rp-address*

Parameter Description

ipv6-rp-address: IPv6 address of a static RP.

acl-name: ACL name that is used to limit address range of multicast groups served by static RPs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If static and dynamic RPs are available at the same time, dynamic RPs are preferred.

If multiple static RPs serve the same multicast group, the static RP with a larger address is preferred.

If the *acl-name* parameter is not specified, the static RPs serve all groups.

Examples

The following example configures the static RP 3333::3333 to serve the multicast group with the address FF66::6666/64 limited by the ACL acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim rp-address 3333::3333 acl
```

Notifications

If the configured RP address is not a valid address, the following notification will be displayed:

```
Illegal RP address, ignored
```

If the number of the RP addresses reaches the upper limit, the following notification will be displayed:

```
Reach PIM-SMv6 static RP configuration limit 65536!
```

If no ACL is configured, the following notification will be displayed:

```
% access-list acl not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode rp mapping**
- **show ipv6 pim sparse-mode rp-hash**

1.27 ipv6 pim rp-candidate

Function

Run the **ipv6 pim rp-candidate** command to configure C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No C-RP is configured by default.

Syntax

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval*] [**group-list** *acl-name*]

no ipv6 pim rp-candidate [*interface-type interface-number*]

default ipv6 pim rp-candidate [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. The address of this interface is specified as the address of a C-RP.

priority *priority-value*: Specifies the C-RP priority. The value range is from 0 to 255, and the default value is **192**.

interval *interval*: Specifies the interval of sending C-RP messages to the BSR, in seconds. The value range is from 1 to 16383, and the default value is **60**.

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups served by a C-RP. The value is a case-sensitive string of 1 to 99 characters. If this parameter is not specified, the C-RP serves all groups.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In PIM-SMv6, an RPT created based on multicast routing takes the RP as a root. After a BSR is elected, all C-RPs periodically send unicast messages to the BSR and then the BSR forwards the messages throughout the PIM domain.

When an ACL is used to specify the address range of groups served by the C-RP, only the permit access control entry (ACE) is calculated, and the deny ACE is not calculated.

Examples

The following example configures the address of GigabitEthernet 0/1 as the C-RP address, sets the RP priority to 200 and the interval of sending C-RP messages to the BSR to 40 seconds, and uses the ACL to limit the address range of groups served by the C-RP to FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim rp-candidate gigabitethernet 0/1 priority 200 group-
list acl interval 40
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

Notifications

If the C-RP priority is not within the range from 0 to 255, the following notification will be displayed:

```
% Invalid C-RP Priority value
```

If the interval of sending C-RP messages to the BSR is not within the range from 1 to 16383 seconds, the following notification will be displayed:

```
% Invalid C-RP advertisement intvl value
```

If the multicast function is not enabled on an interface, the following notification will be displayed:

```
Warning: PIMSMv6 not configured on %s, Candidate-RP not advertised
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ipv6 pim rp-register-kat

Function

Run the **ipv6 pim rp-register-kat** command to configure the (S, G) entry timeout period on an RP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The (S, G) entry timeout period on an RP is the sum of three times of the register suppression time and the register-probe time by default.

Syntax

ipv6 pim rp-register-kat *interval*

no ipv6 pim rp-register-kat

default ipv6 pim rp-register-kat

Parameter Description

Interval: (S, G) entry timeout period on an RP, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The value of the (S, G) entry timeout timer on an RP should be greater than the sum of three times of the register suppression time and the register-probe time on the source DR. Otherwise, the (S, G) on the RP may time out before the source DR sends register messages again, causing a short interrupt of multicast streams.

Examples

The following example sets the (S, G) entry timeout period in register messages to 250 seconds on an RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim rp-register-kat 250
```

Notifications

If the configured (S, G) entry timeout period on an RP is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid KAT value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ipv6 pim rp embedded

Function

Run the **ipv6 pim rp embedded** command to enable the RP address embedding function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

For the IPv6 addresses of multicast groups that support RP address embedding, the RP address embedding function is enabled by default.

Syntax

ipv6 pim rp embedded [**group-list** *acl-name*]

no ipv6 pim rp embedded

default ipv6 pim rp embedded

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** parameter is not specified, the RP address embedding function is enabled on all IPv6 addresses of multicast groups that support RP address embedding.

Examples

The following example enables the RP address embedding function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim rp embedded
```

Notifications

If the group-list is not in the embedded RP linked list, the following notification will be displayed:

```
RP embedded is configured with the same ACL again
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode rp-hash**

1.30 ipv6 pim sparse-mode

Function

Run the **ipv6 pim sparse-mode** command to enable the PIM-SMv6 function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.

The PIM-SMv6 function on an interface is disabled by default.

Syntax

ipv6 pim sparse-mode

no ipv6 pim sparse-mode

default ipv6 pim sparse-mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before PIM-SMv6 is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-SMv6 is enabled.

When PIM-SMv6 is enabled, MLD is automatically enabled on different interfaces.

The multicast function can be enabled on a tunnel interface that does not support multicast. In this case, no notification will be displayed and multicast packets will not be sent or received.

A multicast tunnel cannot be nested and does not support multicast data QoS/ACL.

IPv6 multicast forwarding is not supported on a super VLAN.

Examples

The following example enables the PIM-SMv6 function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode
```

Notifications

If the specified interface does not exist, the following notification will be displayed:

```
ipv6 pim sparse-mode (vif == NULL)
```

If the multicast function is not enabled, the following notification will be displayed:

```
WARNING:  \"ip multicast-routing\"  is not configured
```

If the number of configured multicast interfaces exceeds the upper limit, the following notification will be displayed:

```
PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast routing management)

1.31 ipv6 pim sparse-mode passive

Function

Run the **ipv6 pim sparse-mode passive** command to enable the PIM-SMv6 passive mode on an interface.

Run the **no** form of this command to disable this mode.

Run the **default** form of this command to restore the default configuration.

The PIM-SMv6 mode is disabled on an interface by default.

Syntax

ipv6 pim sparse-mode passive

no ipv6 pim sparse-mode passive

default ipv6 pim sparse-mode passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before the PIM-SMv6 passive mode is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if the PIM-SMv6 passive mode is enabled.

When the PIM-SMv6 mode is enabled, MLD is automatically enabled on different interfaces.

After the PIM-SMv6 passive mode is enabled on an interface, the interface does not receive or send PIM packets, but it can forward multicast packets. It is recommended that the PIM-SMv6 passive mode be enabled on an interface of a stub routing device connected to hosts. This avoids L2 flooding of the PIM hello messages.

Examples

The following example enables the PIM-SMv6 passive mode on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode passive
```

Notifications

N/A

Common Errors

If the PIM-SMv6 passive mode is enabled on an interface connected to a source, the source interface does not send or receive PIM packets. Consequently, the source loses the DR election capability. It is not recommended that the PIM-SMv6 passive mode be enabled on an interface connected to a source.

After the PIM-SMv6 passive mode is enabled on an interface, if two devices in the same network segment forward multicast data, assertion election cannot proceed. As a result, two identical multicast packets are sent to this network segment.

If the PIM-SMv6 passive mode is enabled on an interface of an intermediate device deployed on an L3 multicast network, the networking fails because the interface does not receive or send PIM packets.

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast routing management)

1.32 ipv6 pim spt-threshold

Function

Run the **ipv6 pim spt-threshold** command to enable the shortest path tree (SPT) switchover function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SPT switchover function is disabled by default.

Syntax

ipv6 pim spt-threshold [**group-list** *acl-name*]

no ipv6 pim spt-threshold [**group-list** *acl-name*]

default ipv6 pim spt-threshold [**group-list** *acl-name*]

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of groups that support SPT switchover. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** *acl-name* parameter is not specified, all multicast groups support SPT switchover.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits on the ACL associated with the **group-list** parameter are removed. In this case, all groups are allowed to switch over from an RPT to an SPT.

Examples

The following example uses the ACL acl to set the address range of the multicast source that supports SPT switchover to FE80::2D0:F8FF:FE22:33AD and the address range of the multicast group to FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad/128 ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim spt-threshold group-list acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 ipv6 pim ssm

Function

Run the **ipv6 pim ssm** command to enable the SSM function and configure an SSM group address range.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SSM function is disabled by default.

Syntax

ipv6 pim ssm { **default** | **range** *acl-name* }

no ipv6 pim ssm

default ipv6 pim ssm

Parameter Description

default: Specifies the default SSM group address range to FF3X::/32.

range *acl-name*: Uses an ACL name to limit the SSM group address range. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If SSM needs to be applied in a PIM-SMv6 network, this command must be run.

Examples

The following example enables the SSM function and sets the multicast source address range to FE80::2D0:F8FF:FE22:33AD/128 and the multicast group address range to FF32::3333/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad/128 ff32::3333/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim ssm range acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 mld ssm-map enable** (MLD)
- **ipv6 mld ssm-map static** (MLD)
- **show ipv6 mld ssm-mapping** (MLD)

1.34 ipv6 pim static-rp-preferred

Function

Run the **ipv6 pim static-rp-preferred** command to configure static DR priority to be higher than dynamic RP priority.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Dynamic RP priority is higher than static DR priority by default.

Syntax

ipv6 pim static-rp-preferred

no ipv6 pim static-rp-preferred

default ipv6 pim static-rp-preferred

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the static RP priority is higher than the dynamic DR priority.

Examples

The following example configures static DR priority to be higher than dynamic RP priority.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim static-rp-preferred
```

Notifications

After static DR priority is configured to be higher than dynamic RP priority and RP switchover is performed, the following notification will be displayed.

```
RP is changed for group range %R/%u.  Perform RP change handler
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim rp-address**

1.35 ipv6 pim triggered-hello-delay

Function

Run the **ipv6 pim triggered-hello-delay** command to configure the hello message sending delay on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default hello message sending delay is **5** seconds.

Syntax

ipv6 pim triggered-hello-delay *delay*

no ipv6 pim triggered-hello-delay

default ipv6 pim triggered-hello-delay

Parameter Description

delay: Hello message sending delay, in seconds. The value range is from 1 to 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When an interface is enabled or detects a new neighbor, a random time is generated. Within this time, the interface sends hello messages out.

Examples

The following example sets the hello message sending delay to 3 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim triggered-hello-delay 3
```

Notifications

If the hello message sending delay is not within the range from 1 to 5, the following notification will be displayed:

```
% Invalid Hello option: triggered-hello-delay value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.36 show ipv6 pim sparse-mode bsr-router

Function

Run the **show ipv6 pim sparse-mode bsr-router** command to display BSR information.

Syntax

show ipv6 pim sparse-mode bsr-router

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BSR information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 3333::8888
Uptime:00:03:31, BSR Priority: 64, Hash mask length: 126
Next bootstrap message in 00:00:47
Role: Candidate BSR  Priority: 64, Hash mask length: 126
```

```
State: Elected BSR
Candidate RP: 3333::8888(GigabitEthernet 0/5)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:37
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode bsr-router Command

Field	Description
BSR address	BSR address
Uptime	Update time
BSR Priority	BSR priority
Hash mask length	Hash mask length
Next bootstrap message in *time*	Next bootstrap time
Role	BSR role
Priority	Priority
Hash mask length	Hash mask length
State	BSR status
Candidate RP	C-RP address
Advertisement interval *advertisement-interval* seconds	C-RP advertisement interval
Next Cand_RP_advertisement in *time*	Next C-RP advertisement time

Notifications

N/A

Platform Description

N/A

1.37 show ipv6 pim sparse-mode interface

Function

Run the **show ipv6 pim sparse-mode interface** command to display PIM-SMv6 information of an interface.

Syntax

show ipv6 pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the PIM-SMv6 information of all interfaces is displayed.

detail: Displays the detailed PIM-SMv6 information of an interface. If this parameter is not specified, the summary information of an interface is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SMv6 information of an interface.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode interface detail
GigabitEthernet 0/5 (vif 1):
Address fe80::2d0:f8ff:fe22:33ad, DR fe80::2d0:f8ff:fe22:34b3
Hello period 30 seconds, Next Hello in 6 seconds
Triggered Hello period 5 seconds
Secondary addresses:
   3333::8888
   4444::4444
  Neighbors:
   fe80::2d0:f8ff:fe22:34b3
```

Table 1-2 Output Fields of the show ipv6 pim sparse-mode interface detail Command

Field	Description
Address	Interface address
DR	Address of a DR in the same shared network segment as the interface
Hello period *hello-interval* seconds	Hello message sending interval: *hello-interval* seconds
Next Hello in *next-hello-time* seconds	Next hello message *next-hello-time* seconds later
Triggered Hello period *triggered-hello-time* seconds	Triggered-Hello-Delay of an interface: *triggered-hello-time* seconds
Secondary addresses	Secondary address
Neighbors	Neighbors on an interface

Notifications

N/A

Platform Description

N/A

1.38 show ipv6 pim sparse-mode local-members

Function

Run the **show ipv6 pim sparse-mode local-members** command to display local MLD information of a PIM-SMv6 interface.

Syntax

show ipv6 pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the local MLD information of all PIM-SMv6 interfaces is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays local MLD information of a PIM-SMv6 interface.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/5:
  (*, ff66::6666) : Include
```

Table 1-3 Output Fields of the show ipv6 pim sparse-mode local-members Command

Field	Description
PIM Local membership information	Local member information
interface-type interface-number	Interface type and interface number
(*source*, *ipv6-group-address*): mode	(Multicast source, IPv6 multicast group): source filtering mode

Notifications

N/A

Platform Description

N/A

1.39 show ipv6 pim sparse-mode mroute

Function

Run the **show ipv6 pim sparse-mode mroute** command to display PIM-SMv6 routing information.

Syntax

show ipv6 pim sparse-mode mroute [*ipv6-group-or-source-address* [*ipv6-group-or-source-address*]]

Parameter Description

ipv6-group-or-source-address: Address of an IPv6 multicast group or source (the two addresses cannot be both multicast group addresses or both source addresses).

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Either a source address or a group address can be specified.

A source address and a group address can be specified together.

If you want to configure two addresses, they cannot be both multicast group addresses or both source addresses

If no parameter is specified, all PIM-SMv6 routing information is displayed.

Examples

The following example displays PIM-SMv6 routing information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(*, ff16::1)
RP: 3000::5
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
```

```
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .
i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 44 seconds
kat expires in 194 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .
Outgoing
0  .  .
o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .

(1100::2, ff16::1, rpt)
RP: 3000::5
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. .
```

Table 1-4 Output Fields of the show ipv6 pim sparse-mode mroute Command

Field	Description
IPv6 Multicast Routing Table	IPv6 multicast routing table
(*,*,RP) Entries	Number of (*, *, RP) entries
(*,G) Entries	Number of (*, G) entries
(S,G) Entries	Number of (S, G) entries
(S,G,rpt) Entries	Number of (S, G, RPT) entries
FCR Entries	Number of FCR entries
REG Entries	Number of register entries
RPF nbr	RPF neighbor
RPF idx	RPF interface index

Field	Description
SPT bit	SPT flag bit: 0 or 1 ● **0**: No multicast data is received. ● **1**: Multicast data is received.
Upstream State	Uplink neighbor status includes PRUNED, NOT PRUNED, JOINED, NOT JOINED, PRUNE_PENDING, and RPT NOT JOINED.
jt_timer expires in *jt-expire-time* seconds	Prune expires *jt-expire-time* seconds later.
kat expires in *kat-expire-time* seconds	(S, G) entry expires *kat-expire-time* seconds later.
Local	Inbound interface of a local multicast group
Pruned	Inbound interface for receiving prune packets
Joined	Inbound interface for receiving join packets
Asserted	Inbound interface for receiving assert packets
Outgoing	Outbound interface for forwarding entries

Notifications

N/A

Platform Description

N/A

1.40 show ipv6 pim sparse-mode neighbor

Function

Run the **show ipv6 pim sparse-mode neighbor** command to display neighbor information.

Syntax

show ipv6 pim sparse-mode neighbor [**detail**]

Parameter Description

detail: Displays detailed neighbor information. If this parameter is not specified, the summary information of a neighbor is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays neighbor information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode neighbor detail
Nbr fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5)
 Expires in 86 seconds
  Secondary addresses:
   6666::6666
```

Table 1-5 Output Fields of the show ipv6 pim sparse-mode neighbor detail Command

Field	Description
Nbr	Neighbor information
Expires in *expire-time* seconds	Expiry in *expire-time* seconds
Secondary addresses	Secondary address

Notifications

N/A

Platform Description

N/A

1.41 show ipv6 pim sparse-mode nexthop

Function

Run the **show ipv6 pim sparse-mode nexthop** command to display next hop information, including interface, address, and metric value of a next hop.

Syntax

show ipv6 pim sparse-mode nexthop

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the PIM-SMv6 next hop information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination   Type Nxhp Nexthop                Nexthop                Metrc Pref
Rcnt
                   Num   Addr                  Name
_____________________________________________________________________________
_
100::2       .RS.  1    fe80::21a:a9ff:fe51:2d17 AggregatePort 64.3014   1    110
1
```

Table 1-6 Output Fields of the show ipv6 pim sparse-mode nexthop Command

Field	Description
Destination	Destination address
Type	Type
Nexthop Num	Number of next hops
Nexthop Addr	Next hop address
Nexthop Name	Outbound interface of next hop
Metric	Number of hops to reach the destination address
Pref	Priority of unicast route to reach the destination address
Refcnt	Reference count

Notifications

N/A

Platform Description

N/A

1.42 show ipv6 pim sparse-mode rp mapping

Function

Run the **show ipv6 pim sparse-mode rp mapping** command to display all RPs and the groups served by the RPs on the local device.

Syntax

show ipv6 pim sparse-mode rp mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all RPs and the groups served by the RPs on the local device.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 3333::1
    Info source: 3333::1, via bootstrap, priority 192
        Uptime: 00:12:40, expires: 00:01:50
```

Table 1-7 Output Fields of the show ipv6 pim sparse-mode rp mapping Command

Field	Description
PIM Group-to-RP Mappings	Mapping of PIM RPs to the groups served by the RPs
Group(s)	Address/Mask of a group
RP: *ipv6-rp-address*	RP address: *ipv6-rp-address*
Info source: *ipv6-rp-address*, via bootstrap, priority *priority*	RP address *ipv6-rp-address* is obtained from a BSM, with the priority *priority*.
Uptime	Update time
expires	Expiry time

Notifications

N/A

Platform Description

N/A

1.43 show ipv6 pim sparse-mode rp-hash

Function

Run the **show ipv6 pim sparse-mode rp-hash** command to display RP information corresponding to a multicast group address.

Syntax

show ipv6 pim sparse-mode rp-hash *ipv6-group-address*

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RP information corresponding to a group address FF66::6666.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode rp-hash ff66::6666
 RP: 20::2
Info source: 20::2, via bootstrap

PIMv2 Hash Value 126
RP 20::2, via bootstrap, priority 200, hash value 2007554652
RP 20::1, via bootstrap, priority 200, hash value 844492565
```

Table 1-8 Output Fields of the show ipv6 pim sparse-mode rp-hash Command

Field	Description
RP: *ipv6-rp-address*	Address of the RP serving this multicast group: *ipv6-rp-address*
Info source: *ipv6-rp-address*,via bootstrap	RP address *ipv6-rp-address* is obtained from a BSM.
PIMv2 Hash Value *hash-value*	PIMv2 hash value: *hash-value*
RP *ipv6-rp-address*, via bootstrap, priority *priority* hash value *hash-value*	RP address *ipv6-rp-address* is obtained from a BSM, with the priority *priority* and hash value *hash-value*.

Notifications

N/A

Platform Description

N/A

1.44 show ipv6 pim sparse-mode track

Function

Run the **show ipv6 pim sparse-mode track** command to display the number of PIM packets sent and received since the statistic start time.

Syntax

show ipv6 pim sparse-mode track

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the system is started for the first time, the statistic start time is set. If you run the **clear ipv6 pim sparse-mode track** command, the statistic start time and the PIM packet counter are reset.

Examples

The following example displays the number of PIM packets sent and received since the statistic start time.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode track
PIMv6 packet counters track
Elapsed time since counters cleared: 00:04:03
                    Received   sent
Valid PIMSMv6 packets:  0         8
Hello:                 0         8
Join-Prune:             0         0
Register:              0         0
Register-Stop:          0         0
Assert:                0         0
BSM:                   0         0
C-RP-ADV:               0         0
PIMDMv6-Graft:          0
PIMDMv6-Graft-Ack:      0
PIMDMv6-State-Refresh:  0
```

```
Unknown PIMv6 Type:     0
Errors:
Malformed packets:      0
Bad checksums:          0
Send errors:           0
Packets received with unknown PIMv6 version: 0
```

Table 1-9 Output Fields of the show ipv6 pim sparse-mode track Command

Field	Description
Elapsed time since counters cleared	Duration since the statistic start time till now
Received	Number of received PIM packets
sent	Number of sent PIM packets
Valid PIMSMv6 packets	Valid PIM-SM packets
Hello	Statistical value of hello messages
Join-Prune	Statistical value of join-prune packets
Register	Statistical value of register messages
Register-Stop	Statistical value of register-stop packets
Assert	Statistical value of assert packets
BSM	Statistical value of BSMs
C-RP-ADV	Statistical value of C-RP advertisement packets
PIMDMv6-Graft	Statistical value of PIM-DMv6 graft packets
PIMDMv6-Graft-Ack	Statistical value of PIM-DMv6 graft acknowledgment packets
PIMDMv6-State-Refresh	Statistical value of PIM-DM SRMs
Unknown PIMv6 Type	Unknown PIM packets
Errors	Statistical value of error packets
Malformed packets	Number of malformed packets
Bad checksums	Number of packets with incorrect checksums
Send errors	Number of sent error packets
Packets received with unknown PIMv6 version	Number of PIM packets with unknown version

Notifications

N/A

Platform Description

N/A

1 MLD Snooping Commands

Command	Function
clear ipv6 mld snooping gda-table	Clear Multicast Listener Discovery (MLD) snooping forwarding entries.
clear ipv6 mld snooping statistics	Clear MLD snooping statistics, including the current number of entries, entry capacity, number of different types of packets, group information, and group interface information.
deny	Deny a range of multicast groups specified by a profile.
ipv6 mld profile	Create a profile.
ipv6 mld snooping	Enable MLD snooping globally and set the working mode.
ipv6 mld snooping dyn-mr-aging-time	Configure the aging time of dynamic multicast router ports.
ipv6 mld snooping fast-leave enable	Enable the port fast leave function.
ipv6 mld snooping filter	Enable multicast group filtering on a port.
ipv6 mld snooping host-aging-time	Configure the aging time for MLD snooping dynamic member ports.
ipv6 mld snooping max-groups	Configure the maximum number of multicast groups that can be dynamically learned by a port.
ipv6 mld snooping mrouter learn	Enable the function of dynamic multicast router port learning.
ipv6 mld snooping query-max-response-time	Configure the maximum response time for Query packets.
ipv6 mld snooping source-check port	Enable the source port check function.
ipv6 mld snooping suppression enable	Enable the function of Report packet suppression.
ipv6 mld snooping svgl profile	Specify a range of multicast groups applied in the MLD snooping SVGL mode.
ipv6 mld snooping svgl vlan	Specify the shared VLAN applied in the MLD snooping SVGL mode.
ipv6 mld snooping vlan	Enable the MLD snooping function on a VLAN.

ipv6 mld snooping vlan mrouter interface	Configure a static multicast router port.
ipv6 mld snooping vlan static interface	Configure a static member port.
permit	Permit a range of multicast groups defined by a profile.
range	Define a multicast group range for a profile.
show ipv6 mld profile	Display configurations of a profile.
show ipv6 mld snooping	Display MLD snooping information.
show ipv6 mld snooping gda-table	Display MLD snooping forwarding entries.
show ipv6 mld snooping interfaces	Display multicast filtering configurations on a port.
show ipv6 mld snooping mrouter	Display MLD snooping multicast router ports.
show ipv6 mld snooping statistics	Display MLD snooping statistics.

1.1 clear ipv6 mld snooping gda-table

Function

Run the **clear ipv6 mld snooping gda-table** command to clear Multicast Listener Discovery (MLD) snooping forwarding entries.

Syntax

clear ipv6 mld snooping gda-table

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

An MLD snooping forwarding entry includes the virtual local area network (VLAN) ID, multicast group address, multicast router ports, and member ports.

A VID and multicast group address uniquely identify a forwarding entry.

A forwarding entry may contain multiple multicast router ports, which may be dynamically learned or statically configured. Static multicast router ports never age.

A forwarding entry may contain multiple member ports, which may be dynamically learned or statically configured. Static member ports never age. The **clear ipv6 mld snooping gda-table** command cannot be used to delete static member ports.

Examples

The following example clears MLD snooping multicast forwarding entries.

```
Hostname> enable
Hostname# clear ipv6 mld snooping gda-table
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 mld snooping statistics

Function

Run the **clear ipv6 mld snooping statistics** command to clear MLD snooping statistics, including the current number of entries, entry capacity, number of different types of packets, group information, and group interface information.

Syntax

clear ipv6 mld snooping statistics

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After you run this command, you can run the **show ipv6 mld snooping statistics** command to display the result.

Examples

The following example clears MLD snooping statistics.

```
Hostname> enable
Hostname# clear ipv6 mld snooping statistics
```

Notifications

N/A

Platform Description

N/A

1.3 deny

Function

Run the **deny** command to deny a range of multicast groups specified by a profile.

The deny action is performed for a profile by default.

Syntax

deny

Parameter Description

N/A

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ipv6 mld profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

Examples

The following example denies multicast groups in the range of FF15::1 to FF15::100 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 1
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# deny
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **ipv6 mld profile**
- **permit**
- **range**
- **show ipv6 mld profile**

1.4 ipv6 mld profile

Function

Run the **ipv6 mld profile** command to create a profile.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No profile is configured by default.

Syntax

ipv6 mld profile *profile-number*

no ipv6 mld profile *profile-number*

default ipv6 mld profile *profile-number*

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ipv6 mld profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

Examples

The following example permits multicast groups in the range of FF15::1 to FF15::100 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 1
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# permit
```

Notifications

When a profile fails to be configured, the following notification will be displayed:

```
% Error: configure mld profile fail
```

Platform Description

N/A

Related Commands

- **deny**
- **permit**
- **range**
- **show ipv6 mld profile**

1.5 ipv6 mld snooping

Function

Run the **ipv6 mld snooping** command to enable MLD snooping globally and set the working mode.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

MLD snooping is disabled by default.

Syntax

ipv6 mld snooping { **ivgl** | **svgl** | **ivgl-svgl** }

no ipv6 mld snooping [**ivgl** | **svgl** | **ivgl-svgl**]

default ipv6 mld snooping [**ivgl** | **svgl** | **ivgl-svgl**]

Parameter Description

ivgl: Sets the MLD snooping working mode to Independent VLAN Group Learning (IVGL).

svgl: Sets the MLD snooping working mode to Shared VLAN Group Learning (SVGL).

ivgl-svgl: Sets the MLD snooping working mode to IVGL-SVGL.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In IVGL mode, multicast streams in different VLANs are independent of each other. A host can request only a multicast router port in the same VLAN to receive multicast data. Upon receiving multicast data in any VLAN, the device running MLD snooping forwards the data only to member ports in the same VLAN.

In SVGL mode, hosts in different VLANs share multicast data. Hosts can request multicast data across VLANs. A shared VLAN (VLAN 1 by default) needs to be designated. Only multicast data in the shared VLAN can be forwarded to all member ports of the group address. These member ports can be in other VLANs. A profile must be used to define a range of multicast groups applied in SVGL mode. Only multicast data from this range can be forwarded across VLANs, and other multicast data will be discarded. In IVGL-SVGL mode, the IVGL and SVGL modes coexist. A profile must be used to define a range of multicast groups applied in SVGL mode. Multicast data in this range applies to the SVGL mode, and other multicast data applies to the IVGL mode.

IPv6 multicast data cannot be forwarded in super VLANs.

Examples

The following example enables MLD snooping and runs the IVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping ivgl
```

The following example enables MLD snooping and runs the SVGL mode, sets the shared VLAN to VLAN 1, and sets the multicast groups associated with the SVGL mode to profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping svgl
```

```
Hostname(config)# ipv6 mld snooping svgl profile 1
```

Notifications

When the SVGL or IVGL-SVGL mode is configured before an SVGL profile is configured, the following notification will be displayed:

```
WARNING: Please remember to configure the SVGL profile!
```

Common Errors

The SVGL mode or IVGL-SVGL mode is configured before an SVGL profile is configured. When no SVGL profile is configured, all group information is filtered and no multicast data can be received.

Platform Description

N/A

Related Commands

- **ipv6 mld snooping svgl profile**
- **ipv6 mld snooping svgl vlan**
- **show ipv6 mld snooping**

1.6 ipv6 mld snooping dyn-mr-aging-time

Function

Run the **ipv6 mld snooping dyn-mr-aging-time** command to configure the aging time of dynamic multicast router ports.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default aging time of dynamic multicast router ports is 300s.

Syntax

ipv6 mld snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

no ipv6 mld snooping dyn-mr-aging-time

default ipv6 mld snooping dyn-mr-aging-time

Parameter Description

dynamic-mroute-aging-time: Aging time of dynamic router ports, in seconds. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If a dynamic multicast router port does not receive a general MLD Query packet or a Protocol Independent Multicast (PIM) Hello packet before the aging time, the device deletes the port from the multicast router port list.

When the dynamic multicast router port learning function is enabled, you can run this command to adjust the aging time of dynamic multicast router ports. A too short aging time may cause multicast router ports to be added and deleted frequently.

Dynamic multicast router port learning is enabled by default. If multicast router ports fail to be dynamically learned, run the **show running-config** command to check whether dynamic multicast router port learning is enabled.

Examples

The following example sets the aging time of dynamic multicast router ports to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.7 ipv6 mld snooping fast-leave enable

Function

Run the **ipv6 mld snooping fast-leave enable** command to enable the port fast leave function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The port fast leave function is disabled by default.

Syntax

ipv6 mld snooping fast-leave enable

no ipv6 mld snooping fast-leave enable

default ipv6 mld snooping fast-leave enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the port fast leave function is enabled and a port receives a MLD Done packet, the port is directly deleted from the member port list of the corresponding multicast forwarding entry. When receiving group-specific Query packets, the device does not forward the packets to this port.

The port fast leave function is applicable when only one host is connected to each port. The function helps save bandwidth and resources.

Examples

The following example enables the port fast leave function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping fast-leave enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.8 ipv6 mld snooping filter

Function

Run the **ipv6 mld snooping filter** command to enable multicast group filtering on a port.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The multicast group filtering function is disabled on a port by default.

Syntax

ipv6 mld snooping filter *profile-number*

no ipv6 mld snooping filter

default ipv6 mld snooping filter

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To specify a profile in this command, you must first create the profile.

After this command is configured on a port and the port receives a Report packet from a user host, the device checks whether the multicast address that the user host wants to join is within the multicast group range allowed by the profile. If yes, the user host can join the group. If no, the user host is not allowed to join the group.

Examples

The following example enables multicast group filtering on GigabitEthernet 0/1 and allows user hosts only to join multicast group addresses defined in profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 1
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# permit
Hostname(config-profile)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld snooping filter 1
```

Notifications

N/A

Common Errors

When the configured *profile-number* does not exist, the following notification will be displayed:

```
% Error: The profile doesn't exist
```

When the multicast group filtering function fails to be configured, the following notification will be displayed:

```
% Error: Config interface filter fail, please try again later
```

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping interfaces**

1.9 ipv6 mld snooping host-aging-time

Function

Run the **ipv6 mld snooping host-aging-time** command to configure the aging time for MLD snooping dynamic member ports.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default aging time of dynamic member ports is 260s.

Syntax

ipv6 mld snooping host-aging-time *host-aging-time*

no ipv6 mld snooping host-aging-time

default ipv6 mld snooping host-aging-time

Parameter Description

host-aging-time: Aging time of dynamic member ports, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the device running MLD snooping receives an MLD Join packet from a host to join an IPv6 multicast group, the device adds the port receiving the packet to the member port list and sets an aging time for the port.

If the port is already in the member port list, the device resets the aging timer of the port. The timer time is *host-aging-time*. If the timer times out, it is deemed that no user host receives multicast packets through this port, and then the multicast device deletes the port from the MLD snooping member port list. After this command is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent MLD Join packets. The aging time takes effect immediately after configuration, and the started member port aging timers are updated.

Examples

The following example sets the aging time of MLD dynamic member ports to 30s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping host-aging-time 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.10 ipv6 mld snooping max-groups

Function

Run the **ipv6 mld snooping max-groups** command to configure the maximum number of multicast groups that can be dynamically learned by a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of multicast groups that can be dynamically learned by a port is 64,000 by default.

Syntax

ipv6 mld snooping max-groups *max-groups-number*

no ipv6 mld snooping max-groups

default ipv6 mld snooping max-groups

Parameter Description

max-groups-number: Maximum number of multicast groups. The value range is from 0 to 64000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured and the number of multicast groups dynamically learned by a port exceeds the limit, the device no longer learns MLD Report packets over this port to create new forwarding entries.

The number of multicast groups that can be dynamically learned by a port is counted based on the VLANs to which the port belongs. For example, if a port belongs to three VLANs and the port receives requests of multicast group FF15::100 from each VLAN, the number of multicast groups dynamically learned by the port is 3 instead of 1.

Examples

The following example sets the maximum number of multicast groups that can be dynamically learned by GigabitEthernet 0/1 to **100**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 mld snooping max-groups 100
```

Notifications

When the maximum number of multicast groups that can be dynamically learned by a port fails to be configured, the following notification will be displayed:

```
% Error: Configure interface max-groups fail, please try again later
```

When the number of existing multicast groups exceeds the configured maximum number of multicast groups that can be dynamically learned by a port, the following notification will be displayed:

```
% Warning: The current number(value) is greater than the new interface group
number(value), delete entries related to the interface
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping interfaces**

1.11 ipv6 mld snooping mrouter learn

Function

Run the **ipv6 mld snooping mrouter learn** command to enable the function of dynamic multicast router port learning.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Dynamic multicast router port learning is enabled by default.

Syntax

ipv6 mld snooping [**vlan** *vlan-id*] **mrouter learn**

no ipv6 mld snooping [**vlan** *vlan-id*] **mrouter learn**

default ipv6 mld snooping [**vlan** *vlan-id*] **mrouter learn**

Parameter Description

vlan *vlan-id*: VLAN ID. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A multicast router port is a port that directly connects an MLD snooping-enabled multicast device to a neighbor multicast device in which a multicast routing protocol is enabled. When the dynamic multicast router port learning function is enabled, the device automatically listens to the MLD Query/PIM Hello packets and dynamically identifies a multicast router port.

To dynamically learn multicast router ports, enable the dynamic multicast router port learning function.

To obtain statically configured multicast router ports, run the **ipv6 mld snooping vlan mrouter interface** command.

To disable the dynamic multicast router port learning function for all VLANs, run the **no ipv6 mld snooping mrouter learn** command.

To disable the dynamic multicast router port learning function for a specific VLAN, run the **no ipv6 mld snooping vlan** *vlan-id* **mrouter learn** command.

When the source port check function is enabled, only multicast traffic from the multicast router ports is valid and the multicast device forwards the traffic to registered ports. Multicast data from non-multicast router ports is invalid and will be discarded.

Examples

The following example enables dynamic multicast router port learning only on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping ivgl
Hostname(config)# no ipv6 mld snooping mrouter learn
Hostname(config)# ipv6 mld snooping vlan 1 mrouter learn
```

Notifications

When dynamic multicast router port learning is enabled for a VLAN that does not exist, the following notification will be displayed:

```
% Error: Vlan does not exist
```

When dynamic multicast router port learning is enabled for a VLAN before it is enabled globally, the following notification will be displayed:

```
% Warning: Please remember to enable global mrouter learn
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.12 ipv6 mld snooping query-max-response-time

Function

Run the **ipv6 mld snooping query-max-response-time** command to configure the maximum response time for Query packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum response time for Query packets is 10s by default.

Syntax

ipv6 mld snooping query-max-response-time *query-max-response-time*

no ipv6 mld snooping query-max-response-time

default ipv6 mld snooping query-max-response-time

Parameter Description

query-max-response-time: Maximum response time for Query packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When receiving an MLD group-specific Query packet, the multicast device will start the aging timers of all member ports of the specific group. The timer time is the maximum response time for Query packets. After the timer expires, the device regards that no group member receives multicast traffic through a port and deletes the port from the MLD snooping forwarding table.

For MLDv2 group-specific Query packets, the multicast device does not update the timers.

The configured maximum response time for Query packets takes effect when the next Query packet is received.

Examples

The following example sets the maximum response time for Query packets to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping query-max-response-time 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.13 ipv6 mld snooping source-check port

Function

Run the **ipv6 mld snooping source-check port** command to enable the source port check function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Source port check is disabled by default.

Syntax

ipv6 mld snooping source-check port

no ipv6 mld snooping source-check port

default ipv6 mld snooping source-check port

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source port check function is used to restrict multicast traffic to be forwarded only through multicast router ports. After this function is enabled, only multicast traffic received on multicast router ports is valid. Multicast traffic received on other ports is invalid and will be discarded. If no multicast router port exists in a VLAN, multicast traffic in the VLAN will be discarded.

When the source port check function is disabled, multicast traffic received on any port is valid and will be forwarded to the corresponding member ports.

Examples

The following example enables the source port check function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping source-check port
```

Notifications

If the device does not support the source port check function, the following notification will be displayed:

```
% Error: Device does not support source port check
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.14 ipv6 mld snooping suppression enable

Function

Run the **ipv6 mld snooping suppression enable** command to enable the function of Report packet suppression.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

Report packet suppression is disabled by default.

Syntax

ipv6 mld snooping suppression enable

no ipv6 mld snooping suppression enable

default ipv6 mld snooping suppression enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When Report packet suppression is configured, the MLD multicast device forwards only the first Report packet from a specific VLAN for a multicast group to the multicast router port and suppresses subsequent Report packets for the same multicast group during one query interval. This function helps reduce the number of packets in the network. Only MLDv1 Report packets can be suppressed, and MLDv2 Report packets cannot be suppressed.

Examples

The following example enables the Report packet suppression function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping suppression enable
```

Notifications

When the Report packet suppression function fails to be configured, the following notification will be displayed:

```
% Error: Failed to configure report suppression, please try again
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.15 ipv6 mld snooping svgl profile

Function

Run the **ipv6 mld snooping svgl profile** command to specify a range of multicast groups applied in the MLD snooping SVGL mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No multicast group is configured for the SVGL mode by default.

Syntax

ipv6 mld snooping svgl profile *profile-number*

no ipv6 mld snooping svgl profile

default ipv6 mld snooping svgl profile

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the device running MLD snooping operates in SVGL or IVGL-SVGL mode, the multicast groups associated with the SVGL mode must be configured.

First, define the multicast groups applied in the SVGL mode in a profile. Then, apply this profile in this command.

Examples

The following example applies profile 2 to the SVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 2
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# permit
Hostname(config-profile)# exit
Hostname(config)# ipv6 mld snooping svgl profile 2
```

Notifications

When the configured *profile-number* does not exist, the following notification will be displayed:

```
% Error: The profile doesn't exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 mld profile**
- **ipv6 mld snooping**
- **show ipv6 mld snooping**

1.16 ipv6 mld snooping svgl vlan

Function

Run the **ipv6 mld snooping svgl vlan** command to specify the shared VLAN applied in the MLD snooping SVGL mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default shared VLAN is VLAN 1.

Syntax

ipv6 mld snooping svgl vlan *vlan-id*

no ipv6 mld snooping svgl vlan

default ipv6 mld snooping svgl vlan

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094, and the default value is **1**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the device running MLD snooping operates in SVGL or IVGL-SVGL mode, you can run this command to configure the SVGL shared VLAN.

Examples

The following example sets the shared VLAN applied in SVGL mode to VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping svgl vlan 5
```

Notifications

When the configured *vlan-id* does not exist, the following notification will be displayed:

```
% Error: The vlan does not exist
```

When the configured *vlan-id* is a remote switched port analyzer (SPAN) VLAN, the following notification will be displayed:

```
% Warning: Remote span vlan does not support MLD SNOOPING
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 mld snooping**
- **show ipv6 mld snooping**

1.17 ipv6 mld snooping vlan

Function

Run the **ipv6 mld snooping vlan** command to enable the MLD snooping function on a VLAN.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

When MLD snooping is enabled globally, it takes effect to all VLANs.

Syntax

ipv6 mld snooping vlan *vlan-id*

no ipv6 mld snooping vlan *vlan-id*

default ipv6 mld snooping vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the MLD snooping function in IVGL or IVGL-SVGL mode is enabled globally, you can run the **no ipv6 mld snooping vlan** *vlan-id* command to disable the MLD snooping function on a specific VLAN.

Examples

The following example enables the MLD snooping function in IVGL mode globally and disables the function on VLAN 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping ivgl
Hostname(config)# no ipv6 mld snooping vlan 2
```

Notifications

When the configuration command in SVGL mode is incorrect, the following notification will be displayed:

```
% Error: This command is invalid in SVGL mode
```

When MLD snooping is enabled for a VLAN that does not exist, the following notification will be displayed:

```
% Error: Vlan does not exist
```

When the command is configured on a dynamic VLAN, the following notification will be displayed:

```
% Error: This command does not support dynamic vlan
```

When MLD snooping is enabled on a VLAN before it is enabled globally, the following notification will be displayed:

```
% Warning: Please remember to enable global mld snooping
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping**

1.18 ipv6 mld snooping vlan mrouter interface

Function

Run the **ipv6 mld snooping vlan mrouter interface** command to configure a static multicast router port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static multicast router port is configured by default.

Syntax

ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

default ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

interface-type interface-number: Interface name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To dynamically learn multicast router ports, run the **ipv6 mld snooping vlan mrouter learn** command.

To configure a static multicast router port, run the **ipv6 mld snooping vlan mrouter interface** command. If a port is configured as a static multicast router port, the device can forward all received multicast traffic over this port.

When the source port check function is enabled, only multicast traffic from the multicast router ports is valid and the multicast device forwards the traffic to registered ports. Multicast data from non-multicast router ports is invalid and will be discarded.

Examples

The following example sets the static multicast router port of VLAN 1 to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 0/1
```

Notifications

When a static multicast router port is configured for a VLAN that does not exist, the following notification will be displayed:

```
% Error: Vlan does not exist
```

When the port to be configured as a static multicast router port is an aggregation member port, the following notification will be displayed:

```
% Error: Interface must not be member of aggregateport
```

When the port to be configured as a static multicast router port is not in the corresponding VLAN, the following notification will be displayed:

```
% Error: Interface must be in the vlan you assigned
```

When a static multicast router port fails to be configured, the following notification will be displayed:

```
% Error: Failed to configure static mroute port, please try again
```

When the number of configured static multicast router ports exceeds the limit, the following notification will be displayed:

```
% Error: MLD snooping was trying to configure static mrouter interface than what
allowed (max_num)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping mrouter**

1.19 ipv6 mld snooping vlan static interface

Function

Run the **ipv6 mld snooping vlan static interface** command to configure a static member port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static member port is configured by default.

Syntax

ipv6 mld snooping vlan *vlan-id* **static** *ipv6-group-address* **interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vlan-id* **static** *ipv6-group-address* **interface** *interface-type interface-number*

default ipv6 mld snooping vlan *vlan-id* **static** *ipv6-group-address* **interface** *interface-type interface-number*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

ipv6-group-address: Multicast group address.

interface-type interface-number: Interface name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

An MLD snooping forwarding entry includes the VID, multicast group address, multicast router ports, and member ports.

A VID and multicast group address uniquely identify a forwarding entry.

A forwarding entry may contain multiple multicast router ports, which may be dynamically learned or statically configured. Static multicast router ports never age.

A forwarding entry may contain multiple member ports, which may be dynamically learned or statically configured. Static member ports never age. The **clear ipv6 mld snooping gda-table** command cannot be used to delete static member ports.

Examples

The following example sets the static member port of multicast group FF88::1 in VLAN 1 to GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 mld snooping vlan 1 static FF88::1 interface
gigabitethernet 0/1
```

Notifications

When the multicast group address is invalid, the following notification will be displayed:

```
% Error: Invalid group address
```

When the port to be configured as a static member port is an aggregation member port, the following notification will be displayed:

```
% Error: Interface must not be member of aggregateport
```

When the port to be configured as a static member port is not in the corresponding VLAN, the following notification will be displayed:

```
% Error: Interface must be in the vlan you assigned
```

When a static member port fails to be configured, the following notification will be displayed:

```
% Error: Failed to configure static interface, please try again
```

When the number of configured static member ports exceeds the limit, the following notification will be displayed:

```
% Error: MLD snooping was trying to configure static interface than what allowed
(max_num)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 mld snooping gda-table**

1.20 permit

Function

Run the **permit** command to permit a range of multicast groups defined by a profile.

The deny action is performed for a profile by default.

Syntax

permit

Parameter Description

N/A

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ipv6 mld profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

Examples

The following example permits multicast groups in the range of FF15::1 to FF15::100 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 1
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **deny**
- **ipv6 mld profile**
- **range**
- **show ipv6 mld profile**

1.21 range

Function

Run the **range** command to define a multicast group range for a profile.

Run the **no** form of this command to remove this configuration.

No multicast group range is defined for a profile by default.

Syntax

range *low-ipv6-address* [*high-ipv6-address*]

no range *low-ipv6-address* [*high-ipv6-address*]

Parameter Description

low-ipv6-address: Start IP address of a multicast group range.

high-ipv6-address: End IP address of a multicast group range.

Command Modes

Profile configuration mode

Default Level

14

Usage Guidelines

A profile is a filter for multicast groups and referenced by other functions. To configure a profile, perform the following steps:

(1) Run the **ipv6 mld profile** command to create a profile and enter the profile configuration mode.

(2) Run the **range** command to define a multicast group range.

(3) Run the **permit** or **deny** command to permit or deny the range of multicast groups.

Examples

The following example permits multicast groups in the range of FF15::1 to FF15::100 defined by profile 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 mld profile 1
Hostname(config-profile)# range FF15::1 FF15::100
Hostname(config-profile)# permit
```

Notifications

When *low-ipv6-address* is not a multicast address, the following notification will be displayed:

```
% Error: min_ip(low-ip-address) is not multicast address
```

When *high-ipv6-address* is not a multicast address, the following notification will be displayed:

```
% Error: max_ip(high-ip-address) is not multicast address
```

When *low-ipv6-address* is greater than*high-ipv6-addres*, the following notification will be displayed:

```
% Error: range min_ip(low-ip-address) larger than max_ip(high-ip-address)
```

When the profile to which a multicast group range belongs does not exist, the following notification will be displayed:

```
% Error: The profile doesn't exist
```

When a multicast group range fails to be configured, the following notification will be displayed:

```
% Error: configure profile range fail, please try again
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- deny
- ipv6 mld profile
- permit
- show ipv6 mld profile

1.22 show ipv6 mld profile

Function

Run the **show ipv6 mld profile** command to display configurations of a profile.

Syntax

show ipv6 mld profile [*profile-number*]

Parameter Description

profile-number: Profile ID. The value range is from 1 to 1024. If this parameter is not configured, configurations of all profiles are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about configured profiles. If the *profile-number* parameter is not specified, configurations of all profiles are displayed.

Examples

The following example displays information about all configured profiles.

```
Hostname> enable
Hostname# show ipv6 mld profile
ipv6 mld profile    1
  permit
  range FF15::1 FF15::100
ipv6 mld profile    2
  deny
  range FF88::1  FF88::100
```

Table 1-1 Output Fields of the show ipv6 mld profile Command

Field	Description
profile profile-number	Profile ID
permit/deny	Filtering action of a multicast group range

Field	Description
range *low-ipv6-address high-ipv6-address*	Group range, from the start address to the end address

The following example displays configurations of profile 1.

```
Hostname# show ipv6 mld profile 1
ipv6 mld profile    1
 permit
 range FF15::1 FF15::100
```

Notifications

If you try to query the configuration of a single profile whose *profile-number* has not been configured, the following notification will be displayed:

```
No profile
```

Platform Description

N/A

1.23 show ipv6 mld snooping

Function

Run the **show ipv6 mld snooping** command to display MLD snooping information.

Syntax

show ipv6 mld snooping [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the MLD snooping status and parameters globally or on a specific VLAN.

Examples

The following example displays MLD snooping configurations.

- IVGL mode:

```
Hostname> enable
Hostname# show ipv6 mld snooping
MLD-snooping mode: IVGL
Source port check: Disable
```

```
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Respone Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
vlan 1
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
```

- SVGL mode:

```
Hostname# show ipv6 mld snooping
MLD-snooping mode: SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Respone Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
```

- IVGL-SVGL mode:

```
Hostname# show ipv6 mld snooping
MLD-snooping mode: IVGL-SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Respone Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
vlan 1
----None
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
```

Table 1-2 Output Fields of the show ipv6 mld snooping Command

Field	Description
MLD-snooping mode	Current MLD snooping working mode
Source port check	Whether the source port check function is enabled

Field	Description
MLD Fast-Leave	Whether the fast leave function is enabled
MLD Report suppress	Whether Report packet suppression is enabled
Query Max Response Time	Maximum response time for Query packets
Dynamic Mroute Aging Time	Aging time of dynamic multicast router ports
Dynamic Host Aging Time	Aging time of dynamic member ports
SVGL vlan	Shared VLAN in SVGL or IVGL-SVGL mode
SVGL profile number:	Multicast groups associated with the SVGL or IVGL-SVGL mode
Multicast router learning mode:	Dynamic multicast router port learning
MLD VLAN mode:	VLAN mode

Notifications

N/A

Platform Description

N/A

1.24 show ipv6 mld snooping gda-table

Function

Run the **show ipv6 mld snooping gda-table** command to display MLD snooping forwarding entries.

Syntax

show ipv6 mld snooping gda-table

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays MLD snooping forwarding entries.

```
Hostname> enable
Hostname# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF15::100, 1):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 3/1(SM)
GigabitEthernet 3/7(DSM)
```

Table 1-3 Output Fields of the show ipv6 mld snooping gda-table Command

Field	Description
VLAN	VLAN to which a port belongs
D: DYNAMIC	Dynamic member port
S: STATIC	Static member port
M: MROUTE	Multicast router port

Notifications

N/A

Platform Description

N/A

1.25 show ipv6 mld snooping interfaces

Function

Run the **show ipv6 mld snooping interfaces** command to display multicast filtering configurations on a port.

Syntax

show ipv6 mld snooping interfaces [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is configured, configurations of all ports are displayed.

Examples

The following example displays multicast filtering configurations on a port.

```
Hostname> enable
Hostname# show ipv6 mld snooping interfaces GigabitEthernet 0/1
      Interface            Filter profile number       max-group
GigabitEthernet 0/1          1                        102
Hostname# show ipv6 mld snooping interfaces
      Interface            Filter profile number       max-group
GigabitEthernet 3/1                                   20
```

Table 1-4 Output Fields of the show ipv6 mld snooping interfaces Command

Field	Description
Interface	Interface name.
Filter profile number	Profile referenced for multicast group filtering on a port. If no profile is configured, this parameter is not displayed.
max-group	Maximum number of multicast groups that can be dynamically learned by a port. If this parameter is not configured or is set to the default value, this parameter is not displayed.

Notifications

When configurations of a non-L2 port are queried, the following notification will be displayed:

```
% Error: Interface is not switchport port
```

When configurations of an aggregation member port are queried, the following notification will be displayed:

```
% Error: Interface must not be member of aggregateport
```

Platform Description

N/A

1.26 show ipv6 mld snooping mrouter

Function

Run the **show ipv6 mld snooping mrouter** command to display MLD snooping multicast router ports.

Syntax

show ipv6 mld snooping mrouter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays MLD snooping multicast router ports.

```
Hostname> enable
Hostname# show ipv6 mld snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 2):
  VLAN(2)  1 MROUTES:
GigabitEthernet 3/1(DS)
```

Table 1-5 Output Fields of the show ipv6 mld snooping mrouter Command

Field	Description
VLAN	VLAN to which a port belongs
D: DYNAMIC	Dynamic multicast router port
S: STATIC	Static multicast router port

Notifications

N/A

Platform Description

N/A

1.27 show ipv6 mld snooping statistics

Function

Run the **show ipv6 mld snooping statistics** command to display MLD snooping statistics.

Syntax

show ipv6 mld snooping statistics [**vlan** *vlan-id*]

Parameter Description

vlan *vlan-id*: Specifies a VLAN. The value range is from 1 to 4094. If this parameter is not specified, configurations of all VLANs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays MLD snooping statistics.

```
Hostname> enable
Hostname# show ipv6 mld snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 65536
Current number of MLD Listener Query packet received: 0
Current number of MLDv1 Listener Report packet received: 10
Current number of MLDv2 Listener Report packet received: 0
Current number of MLD Listener Done packet received: 0
Current number of PIM packet received: 0
GROUP     Interface   Reporter        Last join        Last leave   Report pkts
Leave pkts
FF15::1    VL1:Gi0/8   FE80::1         0d:0h:0m:5s       --       1             0
ff15::100  VL1:Gi3/1   --           --             --       0             0
```

Table 1-6 Output Fields of the show ipv6 mld snooping statistics Command

Field	Description
Current number of Gda-table entries	Number of forwarding entries
Configured Statistics database limit	Maximum number of L2 multicast entries
Current number of MLD Listener Query packet received	Number of Query packets received
Current number of MLDv1 Listener Report packet received	Number of MLDv1 Report packets received
Current number of MLDv2 Listener Report packet received	Number of MLDv2 Report packets received
Current number of MLD Listener Done packet received	Number of MLD Done packets received
Current number of PIM packet received	PIM packet data received

Field	Description
GROUP	Group information
Interface	Interface information, which VLAN an interface belongs to
Reporter	Source IP address that sends the last Report packet, which is represented by ---- during static configuration and process restart and restoration
Last join	Interval since the last Report packet is sent, which is represented by ---- during static configuration and process restart and restoration
Last leave	Interval since the last MLD Done packet is sent, which is represented by ---- during static configuration and process restart and restoration
Report pkts	Number of Report packets that are received on a port in a VLAN, which is 0 during static configuration and process restart and restoration
Leave pkts	Number of Leave packets that are received on a port in a VLAN, which is 0 during static configuration and process restart and restoration

Notifications

N/A

Platform Description

N/A

ACL and QoS Commands

1 ACL Commands

Command	Function
access-list	Create an access control list (ACL) and add a rule.
access-list list-remark	Add a remark to an ACL.
access-list remark	Add a remark to an ACL rule.
clear access-list counters	Clear statistics on matched packets denied by an ACL.
clear counters access-list	Clear statistics on the packets matching an ACL.
deny	Add a rule of deny type to an ACL.
expert access-group	Apply an expert ACL.
expert access-list advanced	Create an expert advanced ACL.
expert access-list counter	Enable the packet matching counting function of a specified expert extended ACL.
expert access-list extended	Create an expert extended ACL.
expert access-list new-fragment-mode	Switch the fragmented packet matching mode of an expert extended ACL from the default matching mode to the new matching mode.
expert access-list resequence	Configure the start value and step of rule sequence numbers in an expert extended ACL.
global access-group	Make a global security ACL take effect on a port.
global access-group disable	Disable the global security ACL function.
global ip access-group	Make a global security ACL of IP type take effect on a port.
ip access-group	Apply an IP standard ACL or IP extended ACL.
ip access-list	Create an IP standard ACL or IP extended ACL.
ip access-list counter	Enable the packet matching counting function of an IP standard ACL or IP extended ACL.
ip access-list log-update interval	Configure the update interval of IPv4 ACL packet matching logs.

ip access-list new-fragment-mode	Configure the fragmented packet matching mode of an IP standard ACL or IP extended ACL.
ip access-list resequence	Configure the start value and step of rule sequence numbers in an IP ACL.
ipv6 access-list	Create an IPv6 ACL.
ipv6 access-list counter	Enable the packet matching counting function of an IPv6 ACL.
ipv6 access-list log-update interval	Configure the update interval of IPv6 ACL packet matching logs.
ipv6 access-list resequence	Configure the start value and step of rule sequence numbers in an IPv6 ACL.
ipv6 traffic-filter	Apply an IPv6 ACL.
list-remark	Add a remark to an ACL.
mac access-group	Apply a MAC extended ACL.
mac access-list counter	Enable the packet matching counting function of a MAC extended ACL.
mac access-list extended	Configure a MAC extended ACL.
mac access-list resequence	Configure the start value and step of rule sequence numbers in a MAC extended ACL.
permit	Add a rule of permit type to an ACL.
redirect destination interface	Configure an ACL redirection port.
remark	Add a remark to an ACL rule.
security access-group	Configure a security channel for a port.
security global access-group	Configure a global security channel.
security uplink enable	Configure an excluded port of a global security channel.
show access-group	Display the ACL configuration applied to a port.
show access-lists	Display the configuration of all ACLs or a specified ACL.
show acl res	Display information about all or a specified TCAM.
show acl res detail	Display detailed usage information of all or a specified TCAM.

show expert access-group	Display the configuration of an expert extended ACL applied to a port.
show ip access-group	Display the configuration of IP standard and IP extended ACLs applied to a port.
show ipv6 traffic-filter	Display the configuration of the IPv6 ACL applied to a port.
show mac access-group	Display the MAC extended ACL applied to a port.
show redirect	Display the redirect ACL configuration.
show svi router-acls state	Check whether an ACL applied to an SVI takes effect on L2 and L3 packets.
svi router-acls enable	Enable the function of making an ACL applied to an SVI effective only for L3 forwarded packets.

1.1 access-list

Function

Run the **access-list** command to create an access control list (ACL) and add a rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ACL and its rules are configured by default.

Syntax

The commands for creating ACLs of different types are as follows:

- Create an IP standard ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

- Create an IP extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

Note

The commands for creating IP extended ACLs that specify some important protocols in the protocol field are as follows:

The Transmission Control Protocol (TCP) field is selected.

access-list *acl-number* { **deny** | **permit** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**match-all** *tcp-flag* | **established**] [**time-range** *time-range-name*] [**log**]

- Create a MAC extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

- Create an expert extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  The Ethernet type field or **cos** field is selected.

access-list *acl-number* { **deny** | **permit** } { *ethernet-type* | **cos** [*cos-value*] [**inner** *cos-value*] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

The protocol field is selected.

access-list *acl-number* { **deny** | **permit** } *protocol* [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

Note

The commands for creating expert extended ACLs that specify some important protocols in the protocol field are as follows:

The Internet Control Message Protocol (ICMP) field is selected.

access-list *acl-number* { **deny** | **permit** } **icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The Transmission Control Protocol (TCP) field is selected.

access-list *acl-number* { **deny** | **permit** } **tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The User Datagram Protocol (UDP) field is selected.

access-list *acl-number* { **deny** | **permit** } **udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-*ipv4-*wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

The commands for deleting ACLs of different types are as follows:

no access-list *acl-number*

default access-list *acl-number*

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

deny: Configures the processing action for an ACL rule. If packets match the rule, the packets are denied.

permit: Configures the processing action for an ACL rule. If packets match the rule, the packets are permitted.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence values such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range the L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the type of service (ToS) value of packets. The value range is from 0 to 15. Some important service types such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the differentiated services code point (DSCP) value of packets. The value range is from 0 to 63. Some important differentiated services such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Ethernet protocol type for matching. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To use an ACL to filter data, you must first run the **access-list** command to define a series of ACL rule statements. You can use different kinds of ACLs according to actual needs:

- An IP standard ACL (with the number from 1 to 99 and 1300 to 1999) controls packets based on the source address only.
- An IP extended ACL (with the number from 100 to 199 and 2000 to 2699) implements complex control based on the source and destination addresses.
- A MAC extended ACL (with the number from 700 to 799) performs matching based on the source and destination MAC addresses and Ethernet type.
- An expert extended ACL (with the number from 2700 to 2899) is a combination of the IP standard ACL, IP extended ACL, and MAC extended ACL. You can configure the above three kinds of ACL rules in an expert extended ACL. In addition, the expert extended ACL can also match and filter packets based on the VLAN ID.

Note

For the L3 routing protocols (including the unicast routing protocol and multicast routing protocol), the following parameters are not supported in ACL rules: **precedence** *precedence* / **tos** *tos* / **fragment** / **range** *lower upper* / **time-range** *time-range-name*.

The TCP flag contains some or all of the following bits:

- URG
- ACK
- PSH

- RST
- SYN
- FIN

The packet precedence names are as follows:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service type names are as follows:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The message type names of ICMP packets are as follows:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request

- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The following are TCP port names. A port name or port ID can be used to specify a specific TCP port:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname

- ident
- irc
- klogin
- kshell
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following are UDP port names. A port name or port ID can be used to specify a specific UDP port:

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp

- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The options of **Ethernet-type** are as follows:

- aarp
- arp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

The available protocol layer fields of the UDF header are as follows:

- l2-head
- l3-head
- l4-head
- l5-head
- l6-head

Note

To delete ACL rules, enter the ACL configuration mode and run the **no** { *sequence-number* | **permit** | **deny** } command.

Examples

The following example creates an IP standard ACL and adds a rule: Permit the packets with a source IP address in the range of 192.168.1.64 to 192.168.1.127 to pass through.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

The following example creates an IP extended ACL and adds a rule: Permit the DNS packets and ICMP packets to pass through.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 102 permit tcp any any eq domain log
Hostname(config)# access-list 102 permit udp any any eq domain log
Hostname(config)# access-list 102 permit icmp any any echo log
Hostname(config)# access-list 102 permit icmp any any echo-reply
```

The following example creates a MAC extended ACL and adds a rule: Deny Ethernet frames of the AARP protocol type sent by a source host with the MAC address 00d0.f800.0c0c.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 702 deny host 00d0f8000c0c any aarp
```

The following example creates an expert extended ACL and adds a rule: Deny all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 2702 deny tcp host 192.168.12.3 host 00d0.f800.0044 any
any
Hostname(config)# access-list 2702 permit any any any any
```

Notifications

When a duplicate rule is added to the same ACL, the following notification will be displayed:

```
failed, for the entry is existed or the sequence number has been allocated!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 access-list list-remark

Function

Run the **access-list list-remark** command to add a remark to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL by default.

Syntax

access-list *acl-number* **list-remark** *text*

no access-list *acl-number* **list-remark**

default access-list *acl-number* **list-remark**

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

list-remark *text*: Configures a remark for an ACL. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL conveniently in the future, run this command to add a remark to the ACL. If no ACL exists, this command creates an ACL first and then adds a remark.

Examples

The following example configures an extended ACL numbered 100 and adds the following remark to the ACL: this acl is to filter the host 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip access-list**

1.3 access-list remark

Function

Run the **access-list remark** command to add a remark to an ACL rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL rule by default.

Syntax

access-list *acl-number* **remark** *text*

no access-list *acl-number* **remark** *text*

default access-list *acl-number* **remark** *text*

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

remark *text*: Configures a remark for an ACL rule. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL rule conveniently in the future, run this command to add a remark to the ACL rule.

Examples

The following example configures an ACL numbered 102 and its rule, and then configures the following remark for the ACL rule: deny-host-10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 102 deny ip host 10.1.1.1 host 10.1.1.1
Hostname(config)# access-list 102 remark deny-host-10.1.1.1
```

Notifications

When no rules are configured in an ACL and an ACL rule remark is added, the following notification will be displayed:

```
The ACL has no entry.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 clear access-list counters

Function

Run the **clear access-list counters** command to clear statistics on matched packets denied by an ACL.

Syntax

clear access-list counters [*acl-name* | *acl-number*]

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

To re-collect statistics on matched packets denied by a specified ACL, run this command to clear the statistics on the matched packets denied by the ACL.

Examples

The following example clears statistics on matched packets denied by an ACL numbered 1.

```
Hostname> enable
Hostname# clear access-list counters
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 clear counters access-list

Function

Run the **clear counters access-list** command to clear statistics on the packets matching an ACL.

Syntax

clear counters access-list [*acl-name* | *acl-number*]

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

To re-collect statistics on the packets matching a specified ACL, run this command to clear statistics on packets matching the ACL.

Examples

The following example clears statistics on the packets matching an extended ACL numbered 2700.

```
Hostname> enable
Hostname# clear counters access-list 2700
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 deny

Function

Run the **deny** command to add a rule of deny type to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

There is a rule of deny type in an ACL by default.

Syntax

The commands for adding/deleting a rule of deny type to/from ACLs of different types are as follows:

- IP standard ACL

  Add a rule of deny type to an IP standard ACL.

  [*sequence-number*] **deny** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IP standard ACL.

  no { *sequence-number* | { **deny** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**] } }

- IP extended ACL

  Add a rule of deny type to an IP extended ACL.

  [*sequence-number*] **deny** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IP extended ACL.

  no { *sequence-number* | { **deny** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of deny type to IP extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **deny tcp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] |

[**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **deny udp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- MAC extended ACL

  Add a rule of deny type to a MAC extended ACL.

  [*sequence-number*] **deny** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

  Delete a rule of deny type from a MAC extended ACL.

  no { *sequence-number* | { **deny** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*] } }

- Expert extended ACL

  Add a rule of deny type to an expert extended ACL.

  [*sequence-number*] **deny** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  Delete a rule of deny type from an expert extended ACL.

  no { *sequence-number* | { **deny** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] } }

  The Ethernet type field or **cos** field is selected.

  [*sequence-number*] **deny** { [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

Note

The commands for adding a rule of deny type to expert extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* **| host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The TCP field is selected.

[*sequence-number*] **deny tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The UDP field is selected.

[*sequence-number*] **deny udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source*-ipv4-*wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

- Expert advanced ACL

  Add a rule of deny type to an expert advanced ACL.

  [sequence-number] **deny** hex hex-mask offset

  Delete a rule of deny type from an expert advanced ACL.

  no { sequence-number | **deny** hex hex-mask offset }

- IPv6 extended ACL

  Add a rule of deny type to an IPv6 extended ACL.

  [*sequence-number*] **deny** [*protocol* { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination-mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IPv6 extended ACL.

  no { *sequence-number* | { **deny** [*protocol* { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* **| host** *destination-ipv6-address* | **any** }] [**cos** *cos-value*

[**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of deny type to IPv6 extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **deny tcp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **deny udp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

sequence-number: Sequence number of an ACL rule. The value range is from 1 to 2147483647.

deny: Configures the processing action for an ACL rule. If packets match this rule, the packets are denied.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.0

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence names such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range of L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the ToS value of packets. The value range is from 0 to 15. Some important service type names such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the DSCP value of packets. The value range is from 0 to 63. Some important differentiated service names such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Ethernet protocol type for matching. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

source-ipv6-prefix: Source IPv6 network address or network type for matching.

destination-ipv6-prefix: Destination IPv6 network address or network type for matching.

prefix-length: IPv6 address mask length for matching.

source-ipv6-address: Source IPv6 address for matching.

destination-ipv6-address: Destination IPv6 address for matching.

source-ipv6-mask: Source IPv6 address mask for matching.

destination-ipv6-mask: Destination IPv6 address mask for matching.

flow-label *flow-label*: Matches the flow label value. The value range is from 0 to 1048575.

hex: Matching field in hexadecimal notation. It is used when expert advanced ACL rules are configured.

hex-mask: Matching field mask in hexadecimal notation. It is used when expert advanced ACL rules are configured.

offset: Matching start position, in bytes. It is used when expert advanced ACL rules are configured. The value range is from 0 to 79.

hex hex-mask offset: Combination of *hex*, *hex-mask*, and *offset*. Multiple such combinations can be configured.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To deny some packets access to a network, you can run this command to add rules of deny type to an ACL.

Examples

The following example creates an IP standard ACL and adds a rule: Deny packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard 34
Hostname(config-ext-nacl)# deny host 192.168.4.12
```

The following example creates an IP extended ACL and adds a rule: Deny services provided by the source host with the IP address 192.168.4.12 through TCP port 100.

```
Hostname# configure terminal
Hostname(config)# ip access-list extended ip-ext-acl
Hostname(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
```

The following example creates an expert extended ACL and adds a rule: Deny all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 0013.0049.8272.

```
Hostname# configure terminal
Hostname(config)# expert access-list extended 2702
Hostname(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Hostname(config-exp-nacl)# permit any any any any
```

The following example creates a MAC extended ACL and adds a rule: Deny Ethernet frames of the AARP protocol type sent by the source host with the MAC address 0013.0049.8272.

```
Hostname# configure terminal
Hostname(config)# mac access-list extended mac1
Hostname(config-mac-nacl)# deny host 0013.0049.8272 any aarp
```

The following example creates an IPv6 extended ACL and adds a rule numbered 11: Deny packets sent from the source host with the IP address 2000::1.

```
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-acl)# 11 deny ipv6 host 2000::1 any
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-list** extended
- **ip access-list**
- **ip access-group**
- **mac access-list** extended
- **mac access-group**
- **ipv6 access-list**
- **ipv6 traffic-filter**

1.7 expert access-group

Function

Run the **expert access-group** command to apply an expert ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No expert ACL is applied by default.

Syntax

expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an expert ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert ACL. The value range is from 2700 to 2899.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an expert ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or switch virtual interface (SVI) interface configuration mode. The **counter-only** option is not supported in global configuration mode. The **expert access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the expert extended ACL named accept_00d0f8xxxxxx_only to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-Gigabitethernet 0/1)# expert access-group
accept_00d0f8xxxxxx_only in
```

The following example applies the expert extended ACL numbered 2700 to the inbound direction of the L3 Ethernet interface GigabitEthernet0/1, and collects statistics on the incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# expert access-group 2700 in counter-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-list** advanced
- **expert access-list** extended

1.8 expert access-list advanced

Function

Run the **expert access-list advanced** command to create an expert advanced ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No expert advanced ACL is configured by default.

Syntax

expert access-list advanced *acl-name*

no expert access-list advanced *acl-name*

default expert access-list advanced *acl-name*

Parameter Description

acl-name: Name of an expert advanced ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

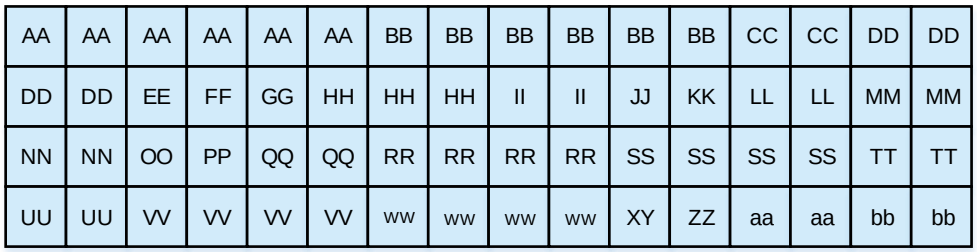
14

Usage Guidelines

To filter packets by user-defined fields, you can use an expert advanced ACL (namely, ACL 80).

Figure 1-1 shows the first 64 bytes of an L2 data frame, where each letter represents one hexadecimal number and every two letters represent one byte.

Figure 1-1 First 64 Bytes of an L2 Data Frame



AA	AA	AA	AA	AA	AA	BB	BB	BB	BB	BB	BB	CC	CC	DD	DD
DD	DD	EE	FF	GG	HH	HH	HH	II	II	JJ	KK	LL	LL	MM	MM
NN	NN	OO	PP	QQ	QQ	RR	RR	RR	RR	SS	SS	SS	SS	TT	TT
UU	UU	VV	VV	VV	VV	ww	ww	ww	ww	XY	ZZ	aa	aa	bb	bb

Table 1-1 lists the offsets of fields in an ACL 80. The offset of each field in the table is their offset in the IEEE 802.3 data frame containing the SNAP+Tag fields.

Table 1-1 Offsets of Fields in an ACL 80

Letter	Description	Offset	Letter	Description	Offset
A	Destination MAC address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number	35
C	Data frame length field	12	Q	IP checksum	36
D	VLAN tag field	14	R	Source IP address	38
E	Destination service access point (DSAP) field	18	S	Destination IP address	42
F	Source service access point (SSAP) field	19	T	TCP source port	46
G	Control field	20	U	TCP destination port	48
H	Org code field	21	V	Serial number	50
I	Encapsulated data type	24	W	Acknowledgment field	54
J	IP version No.	26	XY	IP header length and reserved bits	58
K	ToS field	27	Z	Reserved bits and flags bits	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

Examples

The following example creates an expert advanced ACL named adv-acl.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# expert access-list advanced adv-acl
Hostname(config-exp-dacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-group**

1.9 expert access-list counter

Function

Run the **expert access-list counter** command to enable the packet matching counting function of a specified expert extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an expert extended ACL is disabled by default.

Syntax

expert access-list counter { *acl-name* | *acl-number* }

no expert access-list counter { *acl-name* | *acl-number* }

default expert access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified expert extended ACL, especially to find out whether the network is attacked by a large number of illegitimate packets.

Examples

The following example enables the packet matching counting function of an expert extended ACL named exp-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list counter exp-acl
```

Notifications

When the packet matching counting function of an expert extended ACL is enabled before this ACL is configured, the following notification will be displayed:

```
Create the access-list first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 expert access-list extended

Function

Run the **expert access-list extended** command to create an expert extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No expert extended ACL is configured by default.

Syntax

expert access-list extended { *acl-name* | *acl-number* }

no expert access-list extended { *acl-name* | *acl-number* }

default expert access-list extended { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To achieve the filtering effects of the IP standard ACL, IP extended ACL, and MAC extended ACL in an ACL, configure an expert extended ACL.

Examples

The following example creates an expert advanced ACL named exp-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)#
```

The following example creates an expert extended ACL numbered 2704.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended 2704
Hostname(config-exp-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-group**

1.11 expert access-list new-fragment-mode

Function

Run the **expert access-list new-fragment-mode** command to switch the fragmented packet matching mode of an expert extended ACL from the default matching mode to the new matching mode.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The fragmented packet matching mode of an expert extended ACL is the default matching mode by default.

Syntax

expert access-list new-fragment-mode { *acl-name* | *acl-number* }

no expert access-list new-fragment-mode { *acl-name* | *acl-number* }

default expert access-list new-fragment-mode { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When an ACL rule carries the fragment flag, there is no difference between the default fragmented packet matching mode and the new matching mode.

When an ACL rule does not carry the fragment flag, if the first fragment is required to match all the user-defined matching fields (including L3 and L4 information) in the ACL rule and the non-first fragments need to only match the non-L4 information in the ACL rule, you can run this command to switch the fragmented packet matching mode of the specified ACL to the new matching mode.

Examples

The following example switches the fragmented packet matching mode of an ACL numbered 2700 from the default matching mode to the new matching mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list new-fragment-mode 2700
```

Notifications

When the fragmented packet matching mode of an expert extended ACL is configured before this ACL is configured, the following notification will be displayed:

```
Create the access-list first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 expert access-list resequence

Function

Run the **expert access-list resequence** command to configure the start value and step of rule sequence numbers in an expert extended ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an expert extended ACL are both **10**.

Syntax

expert access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no expert access-list resequence { *acl-name* | *acl-number* }

default expert access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an expert extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an expert extended ACL named exp-acl, and sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list resequence exp-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 global access-group

Function

Run the **global access-group** command to make a global security ACL take effect on a port.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

A port is an excluded port of the global security ACL by default.

Syntax

global access-group

no global access-group

default global access-group

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When a port is an excluded port of the global security ACL and a global security ACL needs to take effect on the port, run this command.

Examples

The following example enables the global security ACL on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# global access-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 global access-group disable

Function

Run the **global access-group disable** command to disable the global security ACL function.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The global security ACL function is enabled by default.

Syntax

global access-group disable

no global access-group disable

default global access-group disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If it is forbidden to configure the global security ACL, disable the global security ACL function. Running this command will delete all global security ACLs.

Examples

The following example disables the global security ACL function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# global access-group disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 global ip access-group

Function

Run the **global ip access-group** command to make a global security ACL of IP type take effect on a port.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

A port is an excluded port of the global security ACL of the IP type by default.

Syntax

global ip access-group

no global ip access-group

default global ip access-group

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When a port is an excluded port of the global security ACL of IP type and a global security ACL of IP type needs to take effect on the port, run this command.

Examples

The following example enables the global security ACL of IP type on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# global ip access-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ip access-group

Function

Run the **ip access-group** command to apply an IP standard ACL or IP extended ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No IP standard ACL or IP extended ACL is applied by default.

Syntax

ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

no ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

default ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

control-plane: Configures a control plane ACL.

counter-only: Configures a special ACL for packet counting on a port.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an IP standard ACL or IP extended ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **ip access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the IP extended ACL numbered 120 to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 120 in
```

The following example applies the IP extended ACL numbered 120 to the inbound direction globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-group 120 in control-plane
```

The following example applies the IP extended ACL numbered 120 to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 120 in counter-only
```

Notifications

When an ACL is applied to the global control plane, if an ACL has been applied to the global control plane, the following notification will be displayed:

```
Another acl has attached at global control-plane, Operation fail
```

When an ACL is applied to a global network segment policy, if an ACL has been applied to the global network segment policy, the following notification will be displayed:

```
Another acl has attached at network-policy, Operation fail
```

When an ACL is applied to a global user group policy, if an ACL has been applied to the global user group policy, the following notification will be displayed:

```
Another acl has attached at user-group-policy, Operation fail
```

When a counter-only ACL is applied to a port, if the counter function of the ACL has been enabled globally, the following notification will be displayed:

```
ACL 1 has been used as a traffic matching statistics ACL.
```

When a counter-only ACL is applied to a port, if an ACL (IP standard ACL, IP extended ACL, MAC extended ACL, or expert ACL) has been applied to the same direction of the port, the following notification will be displayed:

```
Another counter-only acl has attached at GigabitEthernet 0/1, Operation fail.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip access-list**

1.17 ip access-list

Function

Run the **ip access-list** command to create an IP standard ACL or IP extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IP standard ACL or extended ACL is configured by default.

Syntax

ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

no ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

default ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter packets based on the source IP address only, create an IP standard ACL. To control IP packets more finely, for example, filter packets based on the destination IP address or L4 information, create an IP extended ACL. For the matching fields of the two kinds of IP ACLs, refer to the standard and extended forms of the **deny** and **permit** commands. Run the **show access-lists** command to display the ACL configuration.

Examples

The following example creates an IP standard ACL named std-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)#
```

The following example creates an IP extended ACL numbered 123.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 123
Hostname(config-ext-nacl)#
```

Notifications

When you create a named IP standard or IP extended ACL, if the specified name has been used by another type of ACL, the following notification will be displayed:

```
ACL type error, current ACL has been set to type mac extended.
```

When you create a named IP standard or IP extended ACL, if the number of named ACLs (all types of named ACLs) created in the device has reached 500, the following notification will be displayed:

```
Failed to create user-defined acl for the max-limit has been reached
```

When you create a named IP standard or IP extended ACL, if the length of the name entered is longer than 99 characters, the following notification will be displayed:

```
Name is too long
```

When you create a named IP standard or IP extended ACL, if the entered name begins with a number or the name is in or out, the following notification will be displayed:

```
Invalid name
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip access-group**

1.18 ip access-list counter

Function

Run the **ip access-list counter** command to enable the packet matching counting function of an IP standard ACL or IP extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an IP standard ACL or IP extended ACL is disabled by default.

Syntax

ip access-list counter { *acl-name* | *acl-number* }

no ip access-list counter { *acl-name* | *acl-number* }

default ip access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified IP standard ACL or IP extended ACL.

Examples

The following example enables the packet matching counting function of an IP standard ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list counter std-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ip access-list log-update interval

Function

Run the **ip access-list log-update interval** command to configure the update interval of IPv4 ACL packet matching logs.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

Syntax

ip access-list log-update interval *time-value*

no ip access-list log-update interval

default ip access-list log-update interval

Parameter Description

interval *time-value*: Log update interval, in minutes. For the ACL rules with the log output option, it indicates the interval for (in minutes) outputting the ACL matching logs of a data flow. The range is from 0 to 1440. Here, **0** indicates that no ACL matching log is output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

For the IP standard or IP extended ACL rules with the log function enabled, if packets are matched within the log output interval, a log of packet matching count is output when the log output interval expires. To change the log output interval, run this command.

Examples

The following example sets the update interval threshold of IPv4 ACL packet matching logs to 10 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list log-update interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip access-list new-fragment-mode

Function

Run the **ip access-list new-fragment-mode** command to configure the fragmented packet matching mode of an IP standard ACL or IP extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

Syntax

ip access-list new-fragment-mode { *acl-name* | *acl-number* }

no ip access-list new-fragment-mode { *acl-name* | *acl-number* }

default ip access-list new-fragment-mode { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When an ACL rule carries the fragment flag, there is no difference between the default fragmented packet matching mode and the new matching mode.

When the ACL rule does not carry the fragment flag, if the first fragment is required to match all the user-defined matching fields (including L3 and L4 information) in the ACL and the non-first fragments need to only match the non-L4 information in the ACL rule, you can run this command to switch the fragmented packet matching mode of the specified ACL to the new matching mode.

Examples

The following example switches the fragmented packet matching mode of an ACL numbered 100 from the default matching mode to a new matching mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list new-fragment-mode 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip access-list resequence

Function

Run the **ip access-list resequence** command to configure the start value and step of rule sequence numbers in an IP ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an IP ACL are both **10**.

Syntax

ip access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no ip access-list resequence { *acl-name* | *acl-number* }

default ip access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an IP standard ACL or IP extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an IP standard ACL numbered 1, and sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list resequence 1 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ipv6 access-list

Function

Run the **ipv6 access-list** command to create an IPv6 ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IPv6 ACL is configured by default.

Syntax

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

default ipv6 access-list *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter IPv6 packets in the network, run this command to create an IPv6 ACL.

Examples

The following example creates an IPv6 ACL named v6-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 traffic-filter**

1.23 ipv6 access-list counter

Function

Run the **ipv6 access-list counter** command to enable the packet matching counting function of an IPv6 ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an IPv6 ACL is disabled by default.

Syntax

ipv6 access-list counter *acl-name*

no ipv6 access-list counter *acl-name*

default ipv6 access-list counter *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified IPv6 ACL.

Examples

The following example enables the packet matching counting function of an IPv6 ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list counter v6-acl
```

The following example disables the packet matching counting function of an IPv6 ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ipv6 access-list counter v6-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ipv6 access-list log-update interval

Function

Run the **ipv6 access-list log-update interval** command to configure the update interval of IPv6 ACL packet matching logs.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

Syntax

ipv6 access-list log-update interval *time-value*

no ipv6 access-list log-update interval

default ipv6 access-list log-update interval

Parameter Description

interval *time-value*: Log update interval, in minutes. For the ACL rules with the log output option, it indicates the interval for (in minutes) outputting the ACL matching logs of a data flow. The range is from 0 to 1440. Here, **0** indicates that no ACL matching log is output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

For the IPv6 ACL rules with the log function enabled, if packets are matched within the log output interval, a log of packet matching count is output when the log output interval expires. To change the log output interval, run this command.

Examples

The following example sets the update interval of IPv6 ACL packet matching logs to 10 minutes.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 access-list log-update interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ipv6 access-list resequence

Function

Run the **ipv6 access-list resequence** command to configure the start value and step of rule sequence numbers in an IPv6 ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an IPv6 ACL are both **10**.

Syntax

ipv6 access-list resequence *acl-name start-value step-value*

no ipv6 access-list resequence *acl-name*

default ipv6 access-list resequence *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an IPv6 ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an IPv6 ACL named v6-acl, sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list resequence v6-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ipv6 traffic-filter

Function

Run the **ipv6 traffic-filter** command to apply an IPv6 ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No IPv6 ACL is applied by default.

Syntax

ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL only for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an IPv6 ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing IPv6 packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **ipv6 traffic-filter** *acl-name* { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the IPv6 ACL named v6-acl to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

The following example applies the IPv6 ACL named v6-acl to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1, and collects statistics on incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in counter-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 access-list**

1.27 list-remark

Function

Run the **list-remark** command to add a remark to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL by default.

Syntax

list-remark *text*

no list-remark

default list-remark

Parameter Description

text: Remark of an ACL. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL conveniently in the future, run this command to add a remark to the ACL. You can also directly run the **access-list list-remark** command in global configuration mode to add a remark to an ACL.

Examples

The following example adds the following remark to an IP extended ACL numbered 102: this acl is to filter the host 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-list advanced**
- **expert access-list extended**
- **ip access-list**
- **ipv6 access-list**
- **mac access-list extended**

1.28 mac access-group

Function

Run the **mac access-group** command to apply a MAC extended ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No MAC extended ACL is applied by default.

Syntax

mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make a MAC extended ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing Ethernet packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **mac access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the MAC extended ACL named accept_00d0f8xxxxxx_only to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group accept_00d0f8xxxxxx_only
in
```

The following example applies an ACL numbered 700 to the inbound direction of the L3 Ethernet interface GigabitEthernet0/1 and collects statistics on the incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group 700 in counter-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac access-list** extended

1.29 mac access-list counter

Function

Run the **mac access-list counter** command to enable the packet matching counting function of a MAC extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of a MAC extended ACL is disabled by default.

Syntax

mac access-list counter { *acl-name* | *acl-number* }

no mac access-list counter { *acl-name* | *acl-number* }

default mac access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the filtering situation of L2 packets.

Examples

The following example enables the packet matching counting function of a MAC extended ACL named mac-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list counter mac-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 mac access-list extended

Function

Run the **mac access-list extended** command to configure a MAC extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No MAC extended ACL is configured by default.

Syntax

mac access-list extended { *acl-name* | *acl-number* }

no mac access-list extended { *acl-name* | *acl-number* }

default mac access-list extended { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter L2 packets in the network, run this command to create a MAC extended ACL.

Examples

The following example configures a MAC extended ACL named mac-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended mac-acl
Hostname(config-mac-nacl)#
```

The following example configures a MAC extended ACL numbered 704.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended 704
Hostname(config-mac-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **mac access-group**

1.31 mac access-list resequence

Function

Run the **mac access-list resequence** command to configure the start value and step of rule sequence numbers in a MAC extended ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in a MAC extended ACL are both **10**.

Syntax

mac access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no mac access-list resequence { *acl-name* | *acl-number* }

default mac access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into a MAC extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures a MAC extended ACL named mac-acl, sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list resequence mac-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 permit

Function

Run the **permit** command to add a rule of permit type to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

There is no rule of permit type in an ACL by default.

Syntax

The commands for adding/deleting a rule of permit type to/from ACLs of different types are as follows:

- IP standard ACL

  Add a rule of permit type to an IP standard ACL.

  [*sequence-number*] **permit** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

  Delete a rule of permit type from an IP standard ACL.

  no { *sequence-number* | { **permit** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**] } }

- IP extended ACL

  Add a rule of permit type to an IP extended ACL.

  [*sequence-number*] **permit** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

  Delete a rule of permit type from an IP extended ACL.

  no { *sequence-number* | { **permit** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of permit type to IP extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **permit tcp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **permit udp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- MAC extended ACL

  Add a rule of permit type to a MAC extended ACL.

  [*sequence-number*] **permit** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

  Delete a rule of permit type from a MAC extended ACL.

  no { *sequence-number* | { **permit** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*] } }

- Expert extended ACL

  Add a rule of permit type to an expert extended ACL.

  [*sequence-number*] **permit** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  Delete a rule of permit type from an expert extended ACL.

  no { *sequence-number* | { **permit** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] } }

  The Ethernet type or **cos** field is selected.

[*sequence-number*] **permit** { [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

Note

The commands for adding a rule of permit type to expert extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The TCP field is selected.

[*sequence-number*] **permit tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The UDP field is selected.

[*sequence-number*] **permit udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-*ipv4*-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

- Expert advanced ACL

  Add a rule of permit type to an expert advanced ACL.

  [*sequence-number*] **permit** *hex hex-mask offset*

  Delete a rule of permit type from an expert advanced ACL.

  no { *sequence-number* | **permit** *hex hex-mask offset* }

- IPv6 extended ACL

  Add a rule of permit type to an IPv6 extended ACL.

  [*sequence-number*] **permit** [*protocol* { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* |

destination-ipv6-address destination-ipv6-mask | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination-mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

Delete a rule of permit type from an IPv6 extended ACL.

no { *sequence-number* | { **permit** [*protocol* { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of permit type to IPv6 extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **permit tcp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **permit udp** { *source-ipv6-prefix / prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix / prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

sequence-number: Sequence number of an ACL rule. The value range is from 1 to 2147483647.

permit: Configures the processing action for an ACL rule. If packets match this rule, the packets are permitted.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence names such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range of L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the ToS value of packets. The value range is from 0 to 15. Some important service type names such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the DSCP value of packets. The value range is from 0 to 63. Some important differentiated service names such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Matches the Ethernet protocol type. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

source-ipv6-prefix: Source IPv6 network address or network type for matching.

destination-ipv6-prefix: Destination IPv6 network address or network type for matching.

prefix-length: IPv6 address mask length for matching.

source-ipv6-address: Source IPv6 address for matching.

destination-ipv6-address: Destination IPv6 address for matching.

source-ipv6-mask: Source IPv6 address mask for matching.

destination-ipv6-mask: Destination IPv6 address mask for matching.

flow-label *flow-label*: Matches the flow label value. The value range is from 0 to 1048575.

hex: Matching field in hexadecimal notation. It is used when expert advanced ACL rules are configured.

hex-mask: Matching field masks in hexadecimal notation. It is used when expert advanced ACL rules are configured.

offset: Matching start position, in bytes. It is used when expert advanced ACL rules are configured. The value range is from 0 to 79.

hex hex-mask offset: Combination of *hex, hex-mask*, and *offset*. Multiple such combinations can be configured.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To permit some packets to enter a network, you can run this command to add rules of permit type to an ACL.

Examples

The following example creates an IP standard ACL and adds a rule: Permit packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)# permit host 192.168.4.12
```

The following example creates an IP extended ACL and adds a rule: Permit the services provided by the source host with the IP address 192.168.4.12 through TCP port 100.

```
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
```

The following example creates an expert extended ACL and adds a rule: Permit all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 0013.0049.8272.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)# permit tcp host 192.168.4.12 host 0013.0049.8272 any any
Hostname(config-exp-nacl)# deny any any any any
```

The following example creates a MAC extended ACL and adds a rule: Permit the Ethernet frames of the AARP protocol type sent from the source host with the MAC address 0013.0049.8272.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended 702
Hostname(config-mac-nacl)# permit host 0013.0049.8272 any aarp
```

The following example creates an IPv6 extended ACL and adds a rule numbered 11: Permit packets sent from the source host with the IP address 2000::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)# 11 permit ipv6 host 2000::1 any
```

The following example creates an expert advanced ACL and adds a rule: Permit packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list advanced adv-acl
Hostname(config-exp-dacl)# permit c0a8040c ffffffff 38
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-list** extended
- **ip access-list**
- **ip access-group**
- **mac access-list** extended

- **mac access-group**
- **ipv6 access-list**
- **ipv6 traffic-filter**

1.33 redirect destination interface

Function

Run the **redirect destination interface** command to configure an ACL redirection port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ACL redirection port is configured by default.

Syntax

redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

no redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

default redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

Parameter Description

interface *interface-type interface-number*: Interface type and number.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number.

in: Redirects the incoming packets of a port.

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

You can configure a redirect ACL on a port to redirect the incoming packets of the port that match the ACL rules to a specified port. For example, when you need to monitor the running status of an ACL, run this command.

Examples

The following example redirects the incoming packets from the L3 Ethernet interface GigabitEthernet 0/3 that match the rule acl1 to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/3
Hostname(config-if-GigabitEthernet 0/3)# redirect destination interface
gigabitethernet 0/1 acl acl1 in
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 remark

Function

Run the **remark** command to add a remark to an ACL rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL rule by default.

Syntax

[*sequence-number*] **remark** *text*

no [*sequence-number*] **remark** *text*

default [*sequence-number*] **remark** *text*

Parameter Description

sequence-number: Sequence number of an ACL rule, to which a remark needs to be added. The value range is from 1 to 2147483647.

remark *text*: Configures a remark for an ACL rule. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

Two content remarks are forbidden in an ACL rule.

Deleting an ACL rule will delete the rule and its remark.

If the *sequence-number* parameter is specified, the remark is added to the specified ACL rule; if the *sequence-number* parameter is not specified, the remark is added to the last ACL rule.

Examples

The following example adds a remark to an ACL rule in an IP extended ACL numbered 102.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
```

```
Hostname(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Hostname(config-ext-nacl)# remark first_remark
Hostname(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Hostname(config-ext-nacl)# remark second_remark
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **expert access-list** extended
- **ip access-list**
- **ip access-group**
- **mac access-list** extended
- **mac access-group**
- **ipv6 access-list**
- **ipv6 traffic-filter**

1.35 security access-group

Function

Run the **security access-group** command to configure a security channel for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No security channel is configured for a port by default.

Syntax

security access-group { *acl-name* | *acl-number* }

no security access-group

default security access-group

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the authentication function is configured on a device, such as IEEE 802.1x or Web authentication, users must pass the authentication before accessing the external network. To enable users connected to a port to access the external network without undergoing authentication, run this command to configure a security channel.

Examples

The following example configures the ACL numbered 1 as a security channel on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security access-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 security global access-group

Function

Run the **security global access-group** command to configure a global security channel.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No global security channel is configured by default.

Syntax

security global access-group { *acl-name* | *acl-number* }

no security global access-group

default security global access-group

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the authentication function is configured on a device, such as IEEE 802.1x or Web authentication, users must pass the authentication before accessing the external network. To enable users connected to different ports to access the external network without undergoing authentication, run this command to configure a global security channel.

Examples

The following example configures the ACL numbered 1 as a global security channel.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security global access-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 security uplink enable

Function

Run the **security uplink enable** command to configure an excluded port of a global security channel.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No excluded port is configured for a global security channel by default.

Syntax

security uplink enable

no security uplink enable

default security uplink enable

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

The global security channel takes effect on all the ports. To disable the global security channel on some ports, configure these ports as excluded ports of the global security channel.

Examples

The following example configures the L3 Ethernet interface GigabitEthernet 0/1 as an excluded port of a global security channel.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security uplink enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 show access-group

Function

Run the **show access-group** command to display the ACL configuration applied to a port.

Syntax

show access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

To check whether an ACL is applied to a specified port or to find out the ports that have ACLs applied, run this command. If the parameter **interface** is not specified, ACLs applied to all ports are displayed.

Examples

The following example displays information about the ACL applied to a port of the device.

```
Hostname> enable
Hostname# show access-group
ip access-list standard ipstd3 in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out
Applied On interface GigabitEthernet 0/1.
ip access-list extended 101 in
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
Applied On interface GigabitEthernet 0/8.
ipv6 traffic-filter vlan_in in
ipv6 traffic-filter vlan_out out
Applied On vlan 1
```

Table 1-2 Output Fields of the show access-group Command

Field	Description
in	Applied to the inbound direction of a port.
out	Applied to the outbound direction of a port.
Applied On interface X	Applied to interface X.

The following example displays information about the ACL applied to the port GigabitEthernet 0/3.

```
Hostname> enable
Hostname# show access-group interface gigabitethernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

Table 1-3 Output Fields of the show access-group interface Command

Field	Description
in	Applied to the inbound direction of a port.
out	Applied to the outbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.39 show access-lists

Function

Run the **show access-lists** command to display the configuration of all ACLs or a specified ACL.

Syntax

show access-lists [*acl-name* | *acl-number*] [**summary**]

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

summary: Displays the summary of an ACL.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the configuration of a specified ACL. If no ACL number or name is specified, the configuration of all ACLs is displayed.

Examples

The following example displays the configuration of the ACL named n_acl.

```
Hostname> enable
Hostname# show access-lists n_acl
ip access-list standard n_acl
```

The following example displays the configuration of the ACL numbered 102.

```
Hostname# show access-lists 102
ip access-list extended 102
```

The following example displays the configuration of all the ACLs.

```
Hostname> enable
Hostname# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

Table 1-4 Output Fields of the show access-lists Command

Field	Description
ip access-list standard	IP standard ACL.
ip access-list extended	IP extended ACL.
mac access-list extended	MAC extended ACL.
expert access-list extened	Expert extended ACL.
ipv6 access-list extended	IPv6 extended ACL.
permit	Rule of permit type.
deny	Rule of deny type.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.40 show acl res

Function

Run the **show acl res** command to display information about all or a specified TCAM.

Syntax

show acl res [**dev** *dev-number* [**slot** *slot-number*]]

Parameter Description

dev *dev-number*: Displays the TCAM information of a specified device number.

slot *slot-number*: Displays the TCAM information of a specified slot number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the TCAM information of a specified device slot. If no slot number of a device is specified, the TCAM information of all the slots in the device is displayed. If no device number is specified, the TCAM information of all devices is displayed.

Examples

The following example displays the TCAM resources used, usage, and number of remaining entries on all devices.

```
Hostname> enable
Hostname# show acl res
acl usage warn limit: 100%
type          total         used          free          usage
------------   --------      --------      --------      --------
##Dev=1,Slot=0,unit=0 ACL RES
VFP ACL       256           0            256           0%
   slice0     256           0            256           0%
IFP ACL       8000          14           7986          1%
   slice0     2000          14           1986          0%
   slice1     2000          0            2000          0%
   slice2     2000          0            2000          0%
   slice3     2000          0            2000          0%
EFP ACL       1500          0            1500          0%
   slice0     500           0            500           0%
   slice1     500           0            500           0%
   slice2     500           0            500           0%
##Dev=1,Slot=0,unit=0 TOP3
IFP ACL     time:2020/09/25 19:58:35: used=82
```

```
IFP ACL     time:2020/09/25 20:00:05: used=83
IFP ACL     time:2020/09/25 23:45:25: used=84
EFP ACL     time:2020/09/26 12:35:47: used=4
```

Table 1-5 Output Fields of the show acl res dev Command

Field	Description
type	ACL installation stage and slice.
total	Total number of ACLs that can be installed.
used	Number of installed ACLs.
free	Number of remaining ACLs that can be installed.
usage	Usage

The following example displays the TCAM resource used, usage, and number of remaining entries in all slots in device 1.

```
Hostname> enable
Hostname# show acl res dev 1
acl usage warn limit: 100%
type          total         used          free          usage
------------   --------       --------       --------       --------
##Dev=1,Slot=0,unit=0 ACL RES
VFP ACL        256           0             256           0%
   slice0     256           0            256           0%
IFP ACL        8000          14            7986          1%
   slice0     2000          14            1986          0%
   slice1     2000          0             2000          0%
   slice2     2000          0             2000          0%
   slice3     2000          0             2000          0%
EFP ACL        1500          0             1500          0%
   slice0     500           0             500           0%
   slice1     500           0             500           0%
   slice2     500           0             500           0%
##Dev=1,Slot=0,unit=0 TOP3
IFP ACL     time:2020/09/25 19:58:35: used=82
IFP ACL     time:2020/09/25 20:00:05: used=83
IFP ACL     time:2020/09/25 23:45:25: used=84
EFP ACL     time:2020/09/26 12:35:47: used=4
```

Table 1-6 Output Fields of the show acl res dev Command

Field	Description
type	ACL installation stage and slice.

Field	Description
total	Total number of ACLs that can be installed.
used	Number of installed ACLs.
free	Number of remaining ACLs that can be installed.
usage	Usage

Notifications

For the products that share the inter-stage TCAM resources, the displayed resource occupancy at the stages is consistent.

Platform Description

N/A

Related Commands

N/A

1.41 show acl res detail

Function

Run the **show acl res detail** command to display detailed usage information of all or a specified TCAM.

Syntax

show acl res detail [**dev** *dev-number* [**slot** *slot-number*]]

Parameter Description

dev *dev-number*: Displays the detailed usage information of TCAMs in a specified device.

slot *slot-number*: Displays the detailed usage information of the TCAM in a specified slot.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the detailed usage information of the TCAM in a specified device slot. If no slot number of a device is specified, the detailed usage information of TCAMs in all the slots of the device is displayed. If no device number is specified, the detailed usage information of TCAMs in all devices is displayed.

Examples

The following example displays the detailed resource usage of TCAMs in all devices.

```
Hostname> enable
```

```
Hostname# show acl res detail
Dev: 1         Slot: 0       unit: 0              stage: IFP
group id: 2     group pri: 2   total entry: 2000      used entry: 2
width: SINGLE   slice id: 1
app type                    used entry
--------                    ----------
SECURITY-ACL                 2

group id: 1     group pri: 1   total entry: 2000      used entry: 14
width: SINGLE   slice id: 0
app type                    used entry
--------                    ----------
CPP                         14
```

Table 1-7 Output Fields of the show acl res detail Command

Field	Description
group_id	Group ID.
group_pri	Group priority.
total_entry	Number of ACL entries that can be installed.
used_entry	Number of installed ACL entries.
width	Template width.
slice_id	Occupied slice ID.
app_type	Application type.

The following example displays the detailed resource usage of TCAMs in all slots of device 1.

```
Hostname> enable
Hostname# show acl res detail dev 1
Dev: 1         Slot: 0       unit: 0              stage: IFP
group id: 2     group pri: 2   total entry: 2000      used entry: 2
width: SINGLE   slice id: 1
app type                    used entry
--------                    ----------
SECURITY-ACL                 2

group id: 1     group pri: 1   total entry: 2000      used entry: 14
width: SINGLE   slice id: 0
app type                    used entry
--------                    ----------
CPP                         14
```

Table 1-8 Output Fields of the show acl res detail dev Command

Field	Description
group_id	Group ID.
group_pri	Group priority.
total_entry	Number of ACL entries that can be installed.
used_entry	Number of installed ACL entries.
width	Template width.
slice_id	Occupied slice ID.
app_type	Application type.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 show expert access-group

Function

Run the **show expert access-group** command to display the configuration of an expert extended ACL applied to a port.

Syntax

show expert access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the expert ACL applied to a port. If the parameter **interface** is not specified, the expert ACLs applied to all ports are displayed.

Examples

The following example displays information about the expert extended ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show expert access-group interface gigabitethernet 0/1
expert access-group ee in
Applied On interface GigabitEthernet 0/1.
```

Table 1-9 Output Fields of the show expert access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 show ip access-group

Function

Run the **show ip access-group** command to display the configuration of IP standard and IP extended ACLs applied to a port.

Syntax

show ip access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IP standard and IP extended ACLs applied to a port. If the parameter **interface** is not specified, the IP standard and IP extended ACLs applied to all ports are displayed.

Examples

The following example displays information about the IP standard and IP extended ACLs applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Table 1-10 Output Fields of the show ip access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show ipv6 traffic-filter

Function

Run the **show ipv6 traffic-filter** command to display the configuration of the IPv6 ACL applied to a port.

Syntax

show ipv6 traffic-filter [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IPv6 ACL applied to a port. If the parameter **interface** is not specified, the IPv6 ACLs applied to all ports are displayed.

Examples

The following example displays information about the IPv6 ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ipv6 traffic-filter interface gigabitethernet 0/1
ipv6 traffic-filter v6 in
Applied On interface GigabitEthernet 0/1.
```

Table 1-11 Output Fields of the show ipv6 traffic-filter Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show mac access-group

Function

Run the **show mac access-group** command to display the MAC extended ACL applied to a port.

Syntax

show mac access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the MAC extended ACL applied to a port. If the parameter **interface** is not specified, the MAC extended ACLs applied to all ports are displayed.

Examples

The following example displays information about the MAC extended ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac access-group interface gigabitethernet 0/1
mac access-group mm in
Applied On interface GigabitEthernet 0/1.
```

Table 1-12 Output Fields of the show mac access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 show redirect

Function

Run the **show redirect** command to display the redirect ACL configuration.

Syntax

show redirect [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the redirect ACL configuration. If the parameter **interface** is not specified, information about the redirect ACLs configured on all the ports is displayed.

Examples

The following example displays information about the redirect ACL configured on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show redirect interface gigabitethernet 0/1
acl redirect configuration on interface Gigabitethernet 0/1
redirect destination interface Gigabitethernet 0/1 acl 1 in
```

Table 1-13 Output Fields of the show redirect Command

Field	Description
in	Applied to the inbound direction of a port.
redirect destination interface	Destination interface for redirection.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 show svi router-acls state

Function

Run the **show svi router-acls state** command to check whether an ACL applied to an SVI takes effect on L2 and L3 packets.

Syntax

show svi router-acls state

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to check whether an ACL applied to an SVI takes effect on L2 and L3 packets.

Examples

The following example checks whether an ACL applied to an SVI takes effect on L2 and L3 packets.

```
Hostname> enable
Hostname# show svi router-acls state
------------svi router acls state------------
VLAN 2 IN (ip standard 1)
                  L2:enable     L3:enable
```

Table 1-14 Output Fields of the show svi router-acls state Command

Field	Description
IN	Applied to the inbound direction of a port.
L2	Whether it takes effect on L2 packets.
L3	Whether it takes effect on L3 packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 svi router-acls enable

Function

Run the **svi router-acls enable** command to enable the function of making an ACL applied to an SVI effective only for L3 forwarded packets.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of making an ACL applied to an SVI effective only for L3 forwarded packets is disabled by default. Namely, the ACL applied to an SVI is effective for both L2 and L3 forwarded packets.

Syntax

svi router-acls enable

no svi router-acls enable

default svi router-acls enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The ACL applied to an SVI is effective for both L2 and L3 forwarded packets by default. To make the ACL applied to an SVI effective only for the L3 forwarded packets, run this command. This command affects only the ACL applied to an SVI.

Examples

The following example enables the function of making the ACL applied to an SVI effective only for L3 forwarded packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# svi router-acls enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show svi router-acls state**

1 QoS Commands

Command	Function
class	Associate a class with a policy.
class-map	Configure a class.
drop	Configure the traffic behavior of discarding packets.
drr-queue bandwidth	Configure the deficit round robin (DRR) scheduling weights for output queues.
match	Configure a matching rule for a class.
mls qos cos	Configure the IEEE 802.1p value for an interface.
mls qos enable	Enable the global QoS function.
mls qos map cos-dscp	Configure the IEEE 802.1p-to-DSCP mappings for an interface.
mls qos map dscp-cos	Configure the DSCP-to-CoS mappings.
mls qos map ip-precedence-dscp	Configure the IP PRE-to-DSCP mappings.
mls qos scheduler	Configure a scheduling policy for output queues.
mls qos trust	Configure the trust mode for an interface.
police	Configure a bandwidth limit and the traffic behavior of processing packets out of the limit.
policy-map	Configure a policy.
priority-queue	Set the scheduling policy to SP for output queues.
priority-queue cos-map	Configure the CoS-to-queue mappings.
qos queue	Configure the minimum guaranteed bandwidth or maximum limited bandwidth for a queue.
queueing wred	Enable the WRED function.
rate-limit	Configure the rate limit for an interface.
service-policy	Apply a policy.
set	Configure the traffic behavior of modifying a QoS priority.
show class-map	Display information about a class.

show mls qos interface	Display the QoS information of an interface.
show mls qos maps	Display the mappings of different priorities.
show mls qos queueing	Display the CoS-to-queue mappings and the scheduling weights of queues.
show mls qos rate-limit	Display the rate limit information of an interface.
show mls qos scheduler	Display the scheduling policy information of output queues.
show mls qos virtual-group	Display policies associated with a logical interface group.
show policy-map	Display policy information.
show qos bandwidth	Display the queue bandwidth information.
show queueing wred	Display WRED information.
show virtual-group	Display information about members contained in a logical interface group.
virtual-group	Create a logical interface group.
wfq-queue bandwidth	Configure the WFQ scheduling weights for output queues.
wrr-queue bandwidth	Configure the WRR scheduling weights for output queues.
wrr-queue cos-map	Configure the mappings from CoS values to threshold groups.
wrr-queue random-detect min-threshold	Configure the lower threshold value for WRED to discard packets.
wrr-queue random-detect probability	Configure the maximum discarding probability for WRED.

1.1 class

Function

Run the **class** command to associate a class with a policy.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

No class is associated with a policy by default.

Syntax

class *class-map-name*

no class *class-map-name*
default class *class-map-name*

Parameter Description

class *class-map-name*: Configures the name of a class. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

Policy configuration mode

Default Level

14

Usage Guidelines

Before running this command, you must run the **class-map** command to configure a class, run the **policy-map** command to configure a policy, and enter the policy configuration mode.

When multiple classes are associated with the same policy, you are not advised to match the multiple classes with the same flow. Otherwise, the traffic behavior bound to a class takes effect on the flow randomly, and, when the device restarts, the effective traffic behavior may change.

Examples

The following example configures the policy pmap1, associates the class cmap1 with the policy, and enters the policy class configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# class-map cmap1
Hostname(config-cmap)# exit
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cmap1
Hostname(config-pmap-c)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **class-map**
- **policy-map**

1.2 class-map

Function

Run the **class-map** command to configure a class.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No class is configured by default.

Syntax

class-map *class-map-name*

no class-map *class-map-name*

default class-map *class-map-name*

Parameter Description

class-map *class-map-name*: Configures the name of a class. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a class and enter the class configuration mode. You can run the **match** command to configure matching rules for a class.

Examples

The following example configures the class cm_acl and associates the class with an MAC extended access control list (ACL) that permits all the packets with the source MAC address 1111.2222.3333 to pass through.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended me
Hostname(config-ext-macl)# permit host 1111.2222.3333 any
```

```
Hostname(config-ext-macl)# exit
Hostname(config)# class-map cm_acl
Hostname(config-cmap)# match access-group me
```

The following example configures the class cm_dscp for matching packets with the differentiated services code point (DSCP) values 8, 16, and 24.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# class-map cm_dscp
Hostname(config-cmap)# match ip dscp 8 16 24
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **match**

1.3 drop

Function

Run the **drop** command to configure the traffic behavior of discarding packets.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

The traffic behavior of discarding packets is not configured by default.

Syntax

drop

no drop
default drop

Parameter Description

N/A

Command Modes

Policy class configuration mode

Default Level

14

Usage Guidelines

This command can be configured only when no traffic behavior is specified for the class associated with a policy. After the traffic behavior of discarding packets is configured, you need to delete this traffic behavior before configuring other traffic behaviors.

Examples

The following example configures the policy pmap1, associates the class cm-acl with the policy, and configures the traffic behavior of discarding packets in the policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cm-acl
Hostname(config-pmap-c)# drop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **policy-map**
- **class**

1.4 drr-queue bandwidth

Function

Run the **drr-queue bandwidth** command to configure the deficit round robin (DRR) scheduling weights for output queues.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default DRR scheduling weight ratio of output queues is **1:1:1:1:1:1:1:1**.

Syntax

drr-queue bandwidth *weight-value-list*

no drr-queue bandwidth

default drr-queue bandwidth

Parameter Description

weight-value-list: DRR scheduling weights for output queues. The weight value range is from 0 to 15. The value **0** indicates that the SP scheduling policy is used.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the DRR scheduling weights are configured for output queues in both global configuration mode and L2/L3 Ethernet interface configuration mode, the interface configuration prevails.

Examples

The following example sets the DRR scheduling weight ratio to **1:1:1:2:2:4:6:8** for global output queues.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# drr-queue bandwidth 1 1 1 2 2 4 6 8
```

The following example sets the DRR scheduling weight ratio to **1:1:2:2:2:2:4:4** for output queues on L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# drr-queue bandwidth 1 1 2 2 2 2 4 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 match

Function

Run the **match** command to configure a matching rule for a class.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

No matching rules are configured for a class by default.

Syntax

match { **access-group** { *acl-number* | *acl-name* } | **ip** { **dscp** *dscp-value-list* | **precedence** *pre-value-list* } }

no match { **access-group** { *acl-number* | *acl-name* } | **ip** { **dscp** *dscp-value-list* | **precedence** *pre-value-list* } }

Parameter Description

access-group: Matches ACL rules. Both numerically indexed ACLs and named ACLs are supported.

acl-number: Number of a numerically indexed ACL for matching. IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

acl-name: Name of an ACL for matching. The value is a case-sensitive string of 1 to 99 characters.

ip dscp *dscp-value-list*: Matches DSCP rules. Multiple DSCP values can be matched at the same time. The value range is from 0 to 63.

ip precedence *pre-value-list*: Matches IP PRE rules. Multiple IP PRE values can be matched at the same time. The value range is from 0 to 7.

Command Modes

Class configuration mode

Default Level

14

Usage Guidelines

Before running this command, you must run the **class-map** command to configure a class and enter the class configuration mode.

Examples

The following example configures the class cmap1 for matching packets with the IP DSCP values 20, 22, 24, and 30.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# class-map cmap1
Hostname(config-cmap)# match ip dscp 20 22 24 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **class-map**

1.6 mls qos cos

Function

Run the **mls qos cos** command to configure the IEEE 802.1p value for an interface.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default IEEE 802.1p value of an interface is **0**.

Syntax

mls qos cos *cos-value*

no mls qos cos

default mls qos cos

Parameter Description

cos *cos-value*: Configures the IEEE 802.1p value for an interface. The value range is from 0 to 7.

Command Modes

L2 Ethernet interface configuration mode

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the trust mode of an interface is set to untrusted, the packets received from the interface use the IEEE 802.1p value configured for the interface.

Examples

The following example sets the IEEE 802.1p value to **7** for L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabiEthernet 0/1)# mls qos cos 7
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 mls qos enable

Function

Run the **mls qos enable** command to enable the global QoS function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The default configuration of this command depends on the actual product version.

Syntax

mls qos enable

no mls qos enable

default mls qos enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global QoS function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mls qos enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 mls qos map cos-dscp

Function

Run the **mls qos map cos-dscp** command to configure the IEEE 802.1p-to-DSCP mappings for an interface.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The IEEE 802.1p values 0 to 7 of an interface are mapped to DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

Syntax

mls qos map cos-dscp *dscp-value-list*

no mls qos map cos-dscp

default mls qos map cos-dscp

Parameter Description

dscp-value-list: DSCP values, to which IEEE 802.1p values 0 to 7 are to be mapped respectively. The value range is from 0 to 63.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the trust mode of an interface is set to trusting IEEE 802.1p, if a tagged packet of IEEE 802.1q is received from the interface, the IEEE 802.1p value carried in the packet is directly used. If the packet does not carry any tag, the IEEE 802.1p value configured for the interface is used. The mapping table configured using this command and the mapping table configured using the **mls qos map dscp-cos** command are used to jointly obtain CoS values.

Examples

The following example maps IEEE 802.1p values 0 to 7 of an interface to DSCP values 8, 10, 16, 18, 24, 26, 32, and 34 respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mls qos map cos-dscp 8 10 16 18 24 26 32 34
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 mls qos map dscp-cos

Function

Run the **mls qos map dscp-cos** command to configure the DSCP-to-CoS mappings.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

Table 1-1 lists the default mappings from DSCP values to CoS values.

Table 1-1 Default Mappings from DSCP Values to CoS Values

DSCP	CoS Value
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Syntax

mls qos map dscp-cos *dscp-value*&<1-8> **to** *cos-value*

no mls qos map dscp-cos

default mls qos map dscp-cos

Parameter Description

dscp-value&<1-8>: DSCP value. &<1-8> indicates that 1 to 8 DSCP values can be configured. The value range is from 0 to 63.

cos-value: CoS values, to which DSCP values are to be mapped. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

CoS values can be obtained based on DSCP values from the mapping table configured using this command.

Examples

The following example maps DSCP values 8, 10, 16, and 18 to CoS 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 mls qos map ip-precedence-dscp

Function

Run the **mls qos map ip-precedence-dscp** command to configure the IP PRE-to-DSCP mappings.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

IP PRE values 0 to 7 are mapped to DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

Syntax

mls qos map ip-precedence-dscp *dscp-value-list*

no mls qos map ip-precedence-dscp

default mls qos map ip-precedence-dscp

Parameter Description

dscp-value-list: DSCP values, to which IP PRE values 0 to 7 are to be mapped respectively. The value range is from 0 to 63.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the trust mode of an interface is set to trust IP PRE, if a non-IP packet is received from the interface, the packet is processed in the same way of trusting IEEE 802.1p. If an IP packet is received, the CoS value is obtained based on the IP PRE value of the packet from the mapping table configured using this command and the mapping table configured using the **mls qos map dscp-cos** command.

Examples

The following example maps IP PRE values 0 to 7 to DSCP values 8, 10, 16, 18, 24, 26, 32, and 34 respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mls qos map ip-precedence-dscp 8 10 16 18 24 26 32 34
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 mls qos scheduler

Function

Run the **mls qos scheduler** command to configure a scheduling policy for output queues.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

By default, the scheduling policy for global output queues is WRR, and no scheduling policy is configured for the output queues on an interface.

Syntax

mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

no mls qos scheduler

default mls qos scheduler

Parameter Description

drr: Configures DRR scheduling.

rr: Configures round robin (RR) scheduling.

sp: Configures strict priority (SP) scheduling.

wfq: Configures weighted fair queuing (WFQ) scheduling.

wrr: Configures weighted round robin (WRR) scheduling.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

If a scheduling policy is configured for an output queue in both global configuration mode and L2/L3 Ethernet interface configuration mode, the interface configuration prevails.

- In SP scheduling, packets are scheduled strictly based on the queue priorities. Only after all the packets in a queue with a higher priority are processed, can the packets in a queue with a lower priority be processed.
- RR scheduling uses the round robin method to schedule multiple queues. Only one packet in a queue is processed each time.
- WRR scheduling solves the problem that weight cannot be set for RR scheduling. WRR scheduling also adopts the round robin method to schedule multiple queues. The number of packets in a queue processed each time is proportional to the weight of the queue. RR scheduling is equivalent to WRR scheduling with the weight 1.
- DRR scheduling is similar to WRR scheduling, but implements scheduling based on the time slice, instead of the number of packets.
- WFQ scheduling fixes the problem that the queues using WRR scheduling have no fixed egress bandwidth. WFQ scheduling allocates an egress bandwidth to queues based on the queue weight, and different queues can have the opportunity of fair scheduling.

Examples

The following example sets the scheduling policy to SP scheduling for output queues.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mls qos scheduler sp
```

The following example sets the scheduling policy to DRR scheduling for output queues of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mls qos scheduler drr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 mls qos trust

Function

Run the **mls qos trust** command to configure the trust mode for an interface.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default trust mode of an interface is untrusted, and the IEEE 802.1p value configured for the interface is used.

Syntax

mls qos trust { **cos** | **dscp** | **ip-precedence** }

no mls qos trust

default mls qos trust

Parameter Description

cos: Configures trusting IEEE 802.1p.

dscp: Configures trusting DSCP.

ip-precedence: Configures trusting IP PRE.

Command Modes

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the trust mode of L2 Ethernet interface GigabitEthernet 0/1 to trust the IEEE 802.1p value configured for the interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mls qos trust cos
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 police

Function

Run the **police** command to configure a bandwidth limit and the traffic behavior of processing packets out of the limit.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the configuration.

No bandwidth limit and the traffic behavior of processing packets out of the limit are configured by default.

Syntax

police *rate-value burst-value* [**exceed-action** { **cos** *cos-value* [**none-tos**] | **drop** | **dscp** *dscp-value* }]

Parameter Description

rate-value: Rate limit value, in kbps. The value range is from 64 to 33554432.

burst-value: Burst traffic limit value, in Kbytes. The value range is from 4 to 8192.

drop: Discards packets out of the bandwidth limit.

dscp *dscp-value*: Changes the DSCP value of the packets out of the bandwidth limit. The value range is from 0 to 63.

cos *cos-value*: Changes the CoS value of the packets out of the bandwidth limit. The value range is from 0 to 7.

none-tos: Keeps the DSCP value of packets unchanged when the CoS value of packets is changed.

Command Modes

Policy class configuration mode

Default Level

14

Usage Guidelines

After the traffic behavior of discarding packets is configured, you need to delete the configured traffic behavior before configuring the traffic behavior of processing packets out of the limit.

Examples

The following example configures the policy pmap1, associates the class cm-acl with the policy, sets the traffic rate limit to 102400 kbps (namely, 100 Mbps), the burst traffic limit to 4096 Kbytes, and configures the action of changing the DSCP value to 16 for traffic out of the limit.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cm-acl
Hostname(config-pmap-c)# police 102400 4096 exceed-action dscp 16
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **policy-map**
- **class**

1.14 policy-map

Function

Run the **policy-map** command to configure a policy.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No policy is configured by default.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

default policy-map *policy-map-name*

Parameter Description

policy-map *policy-map-name*: Configures a policy name. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Run this command to enter the policy configuration mode. Then, run the **class** command to enter the policy class configuration mode.

Examples

The following example configures the policy po, associates the class cmap1 with the policy, sets the traffic rate limit to 10240 kbps and the burst traffic limit to 256 Kbytes, and configures the action of discarding packets out of the limit in the policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# policy-map po
Hostname(config-pmap)# class cmap1
Hostname(config-pmap-c)# police 10240 256 exceed-action drop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **class**
- **police**

1.15 priority-queue

Function

Run the **priority-queue** command to set the scheduling policy to SP for output queues.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default scheduling policy of output queues is **WRR**.

Syntax

priority-queue

no priority-queue

default priority-queue

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When you run this command to set the scheduling policy to SP for output queues, the effect is the same as that of the **mls qos scheduler sp** command. When you run the **show running-config** command, the **mls qos scheduler sp** command is displayed instead of the **priority-queue** command.

Examples

The following example sets the scheduling policy to SP for output queues.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# priority-queue
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 priority-queue cos-map

Function

Run the **priority-queue cos-map** command to configure the CoS-to-queue mappings.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

CoS values 0 to 7 are mapped to queues 1 to 8 respectively by default.

Syntax

priority-queue cos-map *qid cos-value*&<1-8>

no priority-queue cos-map

default priority-queue cos-map

Parameter Description

qid: Queue ID, to which a CoS value is to be mapped. The value range is from 1 to 8.

cos-value&<1-8>: CoS value to be mapped to a specified queue. &<1-8> means that you can configure the mappings from 1–8 CoS values to queues. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable packets to enter queues based on their CoS values.

Examples

The following example configures mappings from CoS values 3 and 5 to queue 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# priority-queue cos-map 1 3 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 qos queue

Function

Run the **qos queue** command to configure the minimum guaranteed bandwidth or maximum limited bandwidth for a queue.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No minimum guaranteed bandwidth and maximum limited bandwidth are configured for a queue by default.

Syntax

qos queue *queue-id* **bandwidth** { **maximum** *bandwidth* | **minimum** *bandwidth* }

no qos queue *queue-id* **bandwidth** { **maximum** | **minimum** }

default qos queue *queue-id* **bandwidth** { **maximum** | **minimum** }

Parameter Description

queue-id: ID of a queue. The value range is from 1 to 8.

bandwidth maximum *bandwidth*: Configures the maximum limited bandwidth. The value range is from 64 to 10000000.

bandwidth minimum *bandwidth*: Configures the minimum guaranteed bandwidth. The value range is from 64 to 10000000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum limited bandwidth to 10 Mbps and minimum guaranteed bandwidth to 5 Mbps for queue 1 on L2 Ethernet interface GigabitEthernet 0/1, sets the minimum guaranteed bandwidth to 2 Mbps for queue 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth maximum 10240
Hostname(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth minimum 5120
Hostname(config-if-GigabitEthernet 0/1)# qos queue 2 bandwidth minimum 2048
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 queueing wred

Function

Run the **queueing wred** command to enable the WRED function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The WRED function is disabled by default.

Syntax

queueing wred

no queueing wred

default queueing wred

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You need to configure an interface to trust DSCP so that the WRED function takes effect on the interface.

Examples

The following example enables the WRED function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# queueing wred
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 rate-limit

Function

Run the **rate-limit** command to configure the rate limit for an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No rate limit is configured for an interface by default.

Syntax

rate-limit { **input** | **output** } *rate-value burst-value*

no rate-limit { **input** | **output** }

default rate-limit { **input** | **output** }

Parameter Description

input: Limits the traffic in the input direction of an interface.

output: Limits the traffic in the output direction of an interface.

rate-value: Traffic rate limit value, in kbps. The value range is from 64 to 1000000.

burst-value: Burst traffic limit value, in Kbytes. The value range is from 4 to 8192.

Command Modes

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the traffic rate limit to 102400 kbps (namely, 100 Mbps) and burst traffic limit to 2048 Kbytes for L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# rate-limit input 102400 2048
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 service-policy

Function

Run the **service-policy** command to apply a policy.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No policy is applied by default.

Syntax

service-policy { **input** | **output** } *policy-map-name*

no service-policy { **input** | **output** } *policy-map-name*

default service-policy { **input** | **output** } *policy-map-name*

Parameter Description

input: Applies a policy to the input direction of an interface.

output: Applies a policy to the output direction of an interface.

policy-map-name: Name of a policy to be applied. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode

L3 Ethernet interface configuration mode

Logical Interface group configuration mode

Default Level

14

Usage Guidelines

Before running this command, you must run the **policy-map** command to configure a policy.

When policies are applied in both global configuration mode and L2/L3 Ethernet interface configuration mode, the interface configuration prevails.

Examples

The following example applies the policy po to the input direction of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# service-policy input po
```

The following example applies the policy po to the output direction of all the interfaces.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service-policy output po
```

The following example applies the policy po to the output direction of logical interface group 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# virtual-group 3
Hostname(config-VirtualGroup)# service-policy output po
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **virtual-group**

1.21 set

Function

Run the **set** command to configure the traffic behavior of modifying a QoS priority.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

The traffic behavior of modifying a QoS priority is not configured by default.

Syntax

set { **cos** *cos-value* | **ip dscp** *dscp-value* }

no set { **ip dscp** | **cos** }

Parameter Description

cos *cos-value*: Changes the IEEE 802.1p value of an interface. The value range is from 0 to 7.

ip dscp *dscp-value*: Changes the DSCP value. The value range is from 0 to 63.

Command Modes

Policy class configuration mode

Default Level

14

Usage Guidelines

After the traffic behavior of discarding packets is configured, you need to delete the configured traffic behavior before configuring the traffic behavior of modifying a QoS priority.

Examples

The following example configures the policy pmap1, associates the class cmap1 with the policy, and changes the IEEE 802.1p value of packets to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cmap1
Hostname(config-pmap-c)# set cos 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **policy-map**
- **class**

1.22 show class-map

Function

Run the **show class-map** command to display information about a class.

Syntax

show class-map [*class-map-name*]

Parameter Description

class-map-name: Class name. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When no class name is specified, information about all the classes is displayed.

Examples

The following example displays information about all the classes.

```
Hostname> enable
Hostname# show class-map

 Class Map cmap1
   Match ip dscp 20 40
```

```
Class Map cmap2
  Match access-group 110
```

Table 1-2 Output Fields of the show class-map Command

Field	Description
Class Map	Name of a class.
Match	Matching rule.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 show mls qos interface

Function

Run the **show mls qos interface** command to display the QoS information of an interface.

Syntax

show mls qos interface [*interface-type interface-number* | **policers**]

Parameter Description

interface: Displays the QoS information of all the interfaces.

interface-type interface-number: Interface type and interface number. After this parameter is specified, the QoS information of a specified interface is displayed.

policers: Displays the information about policies associated with all the interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *interface-type interface-number* parameter is not specified, the QoS information of all the interfaces is displayed.

Examples

The following example displays the QoS information of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mls qos interface gigabitethernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input: 10240 256
Ratelimit output: 51200 4096
Attached input  policy-map: pmap1
Attached output policy-map:
Default trust: dscp
Default cos: 3
Scheduler type: drr
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
Drr queue bandwidth: 1 1 2 2 2 2 4 4
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Table 1-3 Output Fields of the show mls qos interface Command

Field	Description
Interface	Name of an interface.
Ratelimit input	Rate limit in the input direction of the interface.
Ratelimit output	Rate limit in the output direction of the interface.
Attached input policy-map	Policy associated in the input direction of the interface.
Attached output policy-map	Policy associated in the output direction of the interface.
Default trust	Trust mode of the interface.
Default cos	Default IEEE 802.1p value of the interface.
Scheduler type	Scheduling policy of the interface.
Wrr queue bandwidth	WRR scheduling weights of the output queues of the interface.
Drr queue bandwidth	DRR scheduling weights of the output queues of the interface.
Wfq queue bandwidth	WFQ scheduling weights of the output queues of the interface.

The following example displays information about policies associated with all the interfaces.

```
Hostname> enable
Hostname# show mls qos interface policers
Interface: GigabitEthernet 0/1
Attached input  policy-map: pmap1
Attached output policy-map: pmap1
Interface: GigabitEthernet 0/2
Attached input  policy-map: p1
……
```

Table 1-4 Output Fields of the show mls qos interface policers Command

Field	Description
Interface	Name of an interface.
Attached input policy-map	Policy associated in the input direction of the interface.
Attached output policy-map	Policy associated in the output direction of the interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.24 show mls qos maps

Function

Run the **show mls qos maps** command to display the mappings of different priorities.

Syntax

show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]

Parameter Description

cos-dscp: Displays the IEEE 802.1p-to-DSCP mappings.

dscp-cos: Displays the DSCP-to-CoS mappings.

ip-prec-dscp: Displays the IP PRE-to-DSCP mappings.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When no parameter is specified, the mappings of all the priorities are displayed.

Examples

The following example displays the IEEE 802.1p-to-DSCP mappings.

```
Hostname> enable
Hostname# show mls qos maps cos-dscp
cos dscp
```

```
--- ----
0   0
1   8
2   16
3   24
4   32
5   40
6   48
7   56
```

Table 1-5 Output Fields of the show mls qos maps cos-dscp Command

Field	Description
cos	IEEE 802.1p value of the interface.
dscp	DSCP value, to which an IEEE 802.1p value of the interface is mapped.

The following example displays the DSCP-to-CoS mappings.

```
Hostname> enable
Hostname# show mls qos maps dscp-cos
dscp cos    dscp cos    dscp cos    dscp cos
---- ---    ---- ---    ---- ---    ---- ---
 0   0       1   0       2   0       3   0
 4   0       5   0       6   0       7   0
 8   1       9   1      10   1      11   1
12   1      13   1      14   1      15   1
16   2      17   2      18   2      19   2
20   2      21   2      22   2      23   2
24   3      25   3      26   3      27   3
28   3      29   3      30   3      31   3
32   4      33   4      34   4      35   4
36   4      37   4      38   4      39   4
40   5      41   5      42   5      43   5
44   5      45   5      46   5      47   5
48   6      49   6      50   6      51   6
52   6      53   6      54   6      55   6
56   7      57   7      58   7      59   7
60   7      61   7      62   7      63   7
```

Table 1-6 Output Fields of the show mls qos maps dscp-cos Command

Field	Description
dscp	DSCP value.
cos	CoS value, to which a DSCP value is mapped.

The following example displays the IP PRE-to-DSCP mappings.

```
Hostname> enable
Hostname# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
          0 0
          1 8
          2 16
          3 24
          4 32
          5 40
          6 48
          7 56
```

Table 1-7 Output Fields of the show mls qos maps ip-prec-dscp Command

Field	Description
ip-precedence	IP PRE value.
dscp	DSCP value, to which an IP PRE value is mapped.

The following example displays the DSCP-to-EXP mappings.

```
Hostname> enable
Hostname# show mls qos maps dscp-exp
dscp exp    dscp exp    dscp exp    dscp exp
---- ---    ---- ---    ---- ---    ---- ---
0   0       1   0       2   0       3   0
4   0       5   0       6   0       7   0
8   1       9   1      10   1      11   1
12   1      13   1      14   1      15   1
16   2      17   2      18   2      19   2
20   2      21   2      22   2      23   2
24   3      25   3      26   3      27   3
28   3      29   3      30   3      31   3
32   4      33   4      34   4      35   4
36   4      37   4      38   4      39   4
40   5      41   5      42   5      43   5
44   5      45   5      46   5      47   5
48   6      49   6      50   6      51   6
52   6      53   6      54   6      55   6
56   7      57   7      58   7      59   7
60   7      61   7      62   7      63   7
```

Table 1-8 Output Fields of the show mls qos maps dscp-exp Command

Field	Description

Field	Description
dscp	DSCP value.
exp	EXP value, to which a DSCP value is mapped.

The following example displays the EXP-to-DSCP mappings.

```
Hostname> enable
Hostname# show mls qos maps exp-dscp
exp dscp
--- ----
0   7
1   14
2   21
3   28
4   35
5   42
6   49
7   56
```

Table 1-9 Output Fields of the show mls qos maps exp-dscp Command

Field	Description
exp	EXP value.
dscp	DSCP value, to which an EXP value is mapped.

The following example displays the EXP-to-CoS mappings.

```
Hostname> enable
Hostname# show mls qos maps exp-cos
exp cos
--- ----
0   0
1   1
2   2
3   2
4   2
5   2
6   2
7   7
```

Table 1-10 Output Fields of the show mls qos maps exp-cos Command

Field	Description
exp	EXP value.

Field	Description
cos	CoS value, to which an EXP value is mapped.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.25 show mls qos queueing

Function

Run the **show mls qos queueing** command to display the CoS-to-queue mappings and the scheduling weights of queues.

Syntax

show mls qos queueing [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the information about the specified interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the **interface** *interface-type interface-number* parameter is not specified, the mappings from all the CoS values to queues and the scheduling weights of all the queues are displayed.

Examples

The following example displays the CoS-to-queue mappings and the scheduling weight of queues.

```
Hostname> enable
Hostname# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
```

```
2   3
3   4
4   5
5   6
6   7
7   8

wrr bandwidth weights:
qid weights
--- -------
1   1
2   2
3   3
4   4
5   5
6   6
7   7
8   8

drr bandwidth weights:
qid weights
--- -------
1   3
2   3
3   3
4   3
5   3
6   3
7   3
8   3

wfq bandwidth weights:
qid weights
--- -------
1   3
2   4
3   5
4   6
5   7
6   8
7   9
8   10

Interface: GigabitEthernet 0/1
 Wrr queue bandwidth: 1 1 1 1 2 2 2 2
 Drr queue bandwidth: 1 1 2 2 2 2 4 4
```

```
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Table 1-11 Output Fields of the show mls qos queueing Command

Field	Description
Cos-queue map	CoS-to-queue mappings.
wrr bandwidth weights	WRR scheduling weights of global output queues.
drr bandwidth weights	DRR scheduling weights of global output queues.
wfq bandwidth weights	WFQ scheduling weights of global output queues.
cos	CoS.
qid	Queue ID.
weights	Weight.
Interface	Interface name.
Wrr queue bandwidth	WRR scheduling weights of the output queues of the interface.
Drr queue bandwidth	DRR scheduling weights of the output queues of the interface.
Wfq queue bandwidth	WFQ scheduling weights of the output queues of the interface.

The following example displays the scheduling policy weights of output queues of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mls qos queueing interface gigabitethernet 0/1
Interface: GigabitEthernet 0/1
 Wrr queue bandwidth: 1 1 1 1 2 2 2 2
 Drr queue bandwidth: 1 1 2 2 2 2 4 4
 Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Table 1-12 Output Fields of the show mls qos queueing interface Command

Field	Description
Interface	Interface name.
Wrr queue bandwidth	WRR scheduling weights of the output queues of the interface.
Drr queue bandwidth	DRR scheduling weights of the output queues of the interface.
Wfq queue bandwidth	WFQ scheduling weights of the output queues of the interface.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show mls qos rate-limit

Function

Run the **show mls qos rate-limit** command to display the rate limit information of an interface.

Syntax

show mls qos rate-limit [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the rate limit information of a specified interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, the rate limit information of all the interfaces is displayed.

Examples

The following example displays the rate limit information of all the interfaces.

```
Hostname> enable
Hostname# show mls qos rate-limit
Interface: GigabitEthernet 0/1
  rate limit input Kbps = 10240 burst = 256
```

Table 1-13 Output Fields of the show mls qos rate-limit Command

Field	Description
Interface	Interface name.
rate limit input Kbps = x burst = y	The bandwidth limit per second in the input direction of the interface is x kbps, and the burst traffic limit value is y Kbytes per second.
rate limit output Kbps = x burst = y	The bandwidth limit per second in the output direction of the interface is x kbps, and the burst traffic limit is y Kbytes per second.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show mls qos scheduler

Function

Run the **show mls qos scheduler** command to display the scheduling policy information of output queues.

Syntax

show mls qos scheduler [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the scheduling policy information of the output queues of a specified interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, the scheduling policy information of the global output queues is displayed.

Examples

The following example displays the scheduling policy information of global output queues.

```
Hostname> enable
Hostname# show mls qos scheduler
Global Multi-Layer Switching scheduling
 Weighted Round Robin
Interface GigabitEthernet 0/1 Multi-Layer Switching scheduling:
 Deficit Round Robin
```

Table 1-14 Output Fields of the show mls qos scheduler Command

Field	Description
Weighted Round Robin	The queue scheduling policy is WRR, and the other types of scheduling policies are as follows: ● SP ● RR ● WFQ ● DRR
Interface	Interface name

The following example displays the scheduling policy of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mls qos scheduler interface gigabitethernet 0/1
Interface GigabitEthernet 0/1 Multi-Layer Switching scheduling:
 Deficit Round Robin
```

Table 1-15 Output Fields of the show mls qos scheduler interface Command

Field	Description
Interface	Interface name.
Deficit Round Robin	The scheduling policy of the interface is DRR.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show mls qos virtual-group

Function

Run the **show mls qos virtual-group** command to display policies associated with a logical interface group.

Syntax

show mls qos virtual-group [*virtual-group-number* | **policers**]

Parameter Description

virtual-group-number: Number of a logical interface group. After this parameter is specified, policies associated with a specified logical interface group are displayed. The value range is from 1 to 128.

policers: Displays the policies associated with all the logical interface groups.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *virtual-group-number* parameter is not specified, policies associated with all the logical interface groups are displayed.

Examples

The following example displays policies associated with all the logical interface groups.

```
Hostname> enable
Hostname# show mls qos virtual-group policers
Virtual-group: 1
Attached input policy-map: pmap1
Virtual-group: 20
Attached output policy-map: pmap2
```

Table 1-16 Output Fields of the show mls qos virtual-group policers Command

Field	Description
Virtual-group	Number of a logical Interface group.
Attached input policy-map	Policy applied to the input direction of the logical interface group.
Attached output policy-map	Policy applied to the output direction of the logical interface group.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show policy-map

Function

Run the **show policy-map** command to display policy information.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

Parameter Description

policy-map-name: Name of a policy. The value is a case-sensitive string of 1 to 31 characters.

class *class-map-name*: Name of the class associated with the policy. The value is a case-sensitive string of 1 to 31 characters.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *policy-map-name* parameter is not specified, information about all the policies is displayed.

Examples

The following example displays information about policy pmap1.

```
Hostname> enable
Hostname# show policy-map pmap1

 Policy Map pmap1
   Class cmap1
     set ip dscp 16
   Class cmap2
     police 10240 256 exceed-action dscp 8
   Class cmap3
     police 512000 4096 exceed-action drop
```

Table 1-17 Output Fields of the show policy-map Command

Field	Description
Policy Map	Name of a policy.
Class	Name of a class associated with the policy.
set	The bound traffic behavior is modifying the 802.1p and DSCP.
police	The bound traffic behavior is limiting the bandwidth and processing packets out of the limit.

The following example displays the policy pmap1, in which the traffic behavior bound to the class cmap1 is associated.

```
Hostname> enable
Hostname# show policy-map pmap1 class cmap1

   Class cmap1
     set ip dscp 16
```

Table 1-18 Output Fields of the show policy-map class Command

Field	Description
Class	Name of a class associated with the policy.
set	The bound traffic behavior is modifying the 802.1p and DSCP.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 show qos bandwidth

Function

Run the **show qos bandwidth** command to display the queue bandwidth information.

Syntax

show qos bandwidth [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the queue bandwidth information of a specified interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, bandwidth information of all the queues is displayed.

Examples

The following example displays the bandwidth information of L2 Ethernet interface GigabitEthernet 0/1. The following information is displayed only for device interfaces that support separate configuration of bandwidths of unicast queues and multicast queues.

```
Hostname> enable
Hostname# show qos bandwidth interface gigabitethernet 0/1

Interface: GigabitEthernet 0/1
 ---------------------------------------------------
 uc-queue-id | minimum-bandwidth | maximum-bandwidth
 -----------   -----------------   -----------------
         1              5120             10240
         2                 0                 0
         3                 0                 0
         4                 0                 0
         5                 0                 0
         6                 0                 0
         7                 0                 0
         8                 0                 0
 ---------------------------------------------------
 Total ucast-queue minimum-bandwidth:          5120
 Total ucast-queue maximum-bandwidth:         10240

Interface: GigabitEthernet 0/1
 ---------------------------------------------------
 mc-queue-id | minimum-bandwidth | maximum-bandwidth
 -----------   -----------------   -----------------
         1              1024              5120
         2                 0                 0
         3                 0                 0
         4                 0              2048
 ---------------------------------------------------
 Total mcast-queue minimum-bandwidth:          1024
Total mcast-queue maximum-bandwidth:          5120
```

Table 1-19 Output Fields of the show qos bandwidth interface Command

Field	Description
Interface	Name of an interface.
queue-id	Queue ID. It is displayed when the bandwidth of unicast and multicast queues is configured together.
uc-queue-id	Unicast queue ID. It is displayed when the bandwidth of unicast queues is configured separately.

Field	Description
mc-queue-id	Multicast queue ID. It is displayed when the bandwidth of multicast queues is configured separately.
minimum-bandwidth	Minimum guaranteed bandwidth, in Kbytes per second.
maximum-bandwidth	Maximum limited bandwidth, in Kbytes per second.
Total queue minimum-bandwidth	Sum of the minimum guaranteed bandwidths configured for all the queues. It is displayed when the bandwidth of unicast and multicast queues is configured together.
Total queue maximum-bandwidth	Sum of the maximum limited bandwidths configured for all the queues. It is displayed when the bandwidth of unicast and multicast queues is configured together.
Total ucast-queue minimum-bandwidth	Sum of the minimum guaranteed bandwidths configured for all the unicast queues. It is displayed when the bandwidth of unicast queues is configured separately.
Total ucast-queue maximum-bandwidth	Sum of the maximum limited bandwidths configured for all the unicast queues. It is displayed when the bandwidth of unicast queues is configured separately.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.31 show queueing wred

Function

Run the **show queueing wred** command to display WRED information.

Syntax

show queueing wred [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Displays the WRED information of a specified interface type and number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, the WRED information configured for all the interfaces is displayed.

Examples

The following example displays the WRED information configured for L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show queueing wred interface gigabitethernet 0/1
---  --------- ---------- ----- ----- ------  --------- ---------- ----- ----- ------
qid  max_cell_1 min_cell 1 max_1 min_1 prob_1 max_cell_2 min_cell 2  max_2 min_2 prob_2
---  --------- ---------- ----- ----- ------  --------- ---------- ----- ----- ------
1    120000     120000    100   30    100    120000     120000     100   70    100
2    120000     120000    100   60    100    120000     120000     100   30    100
3    120000     120000    100   80    30     120000     120000     100   30    40
4    120000     120000    100   80    100    120000     120000     100   100   100
5    120000     120000    100   80    100    120000     120000     100   100   100
6    120000     120000    100   80    100    120000     120000     100   100   100
7    120000     120000    100   80    100    120000     120000     100   100   100
8    120000     120000    100   80    100    120000     120000     100   100   100



---  ---  ------------
cos  qid  threshold_id
---  ---  ------------
0    1    1
1    2    2
2    3    2
3    4    2
4    5    2
5    6    1
6    7    1
7    8    1
```

Table 1-20 Output Fields of the show queueing wred interface Command

Field	Description
qid	Queue ID.
max_cell_x	Higher threshold value of group x, in the unit of cell.
min_cell_x	Lower threshold value of group x, in the unit of cell.
max_x	Higher threshold value of group x, in percentage.

Field	Description
min_x	Lower threshold value of group x, in percentage.
prob_x	Maximum discarding probability of group x.
cos qid threshold_id	CoS-to-queue mapping and CoS-to-threshold group mapping.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.32 show virtual-group

Function

Run the **show virtual-group** command to display information about members contained in a logical interface group.

Syntax

show virtual-group [*virtual-group-number* | **summary**]

Parameter Description

virtual-group-number: Number of a logical interface group. After this parameter is specified, information about members contained in a specified logical interface group is displayed. The value range is from 1 to 128.

summary: Displays information about members contained in all the logical interface groups.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the *virtual-group-number* parameter is not specified, information about members contained in all the logical interface groups is displayed.

Examples

The following example displays information about members contained in all the logical interface groups.

```
Hostname> enable
Hostname# show virtual-group summary
```

```
virtual-group       member
-------------       ------------------------
1                    Gi0/1 Gi0/2
2                    Gi0/0
```

Table 1-21 Output Fields of the show virtual-group summary Command

Field	Description
virtual-group	Number of a logical Interface group.
member	Member interface in the logical interface group.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.33 virtual-group

Function

Run the **virtual-group** command to create a logical interface group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No logical interface group is created by default.

Syntax

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

default virtual-group *virtual-group-number*

Parameter Description

virtual-group-number: Number of a logical interface group. The value range is from 1 to 128.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

In the global configuration mode, you can run this command to create a logical interface group and enter the logical interface group configuration mode.

In the L2/L3 Ethernet interface configuration mode, you can run this command to add the interface to a logical interface group. If the logical interface group is created, this command creates the logical interface group and adds the interface to the logical interface group.

Members to be added to a logical interface group must be physical interfaces or aggregation ports. The members of a logical interface group must be in the same line card or the same device.

Examples

The following example adds L2 Ethernet interface GigabitEthernet 0/1 to logical interface group 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# virtual-group 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 wfq-queue bandwidth

Function

Run the **wfq-queue bandwidth** command to configure the WFQ scheduling weights for output queues.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default WFQ scheduling weight ratio of output queues is **1:1:1:1:1:1:1:1**.

Syntax

wfq-queue bandwidth *weight-value-list*

no wfq-queue bandwidth

default wfq-queue bandwidth

Parameter Description

weight-value-list: WFQ scheduling weights for output queues. The weight value range is from 0 to 15. The value **0** indicates that the SP scheduling policy is used.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the WFQ scheduling weights are configured for output queues in both global configuration mode and L2/L3 Ethernet interface configuration mode, the interface configuration prevails.

Examples

The following example sets the WFQ scheduling weight ratio of global output queues to **1:1:2:4:4:4:6:8**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# wfq-queue bandwidth 1 1 2 4 4 4 6 8
```

The following example sets the WFQ scheduling weight ratio of output queues on L2 Ethernet interface GigabitEthernet 0/1 to **1:1:2:2:2:2:4:4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# wfq-queue bandwidth 1 1 2 2 2 2 4 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 wrr-queue bandwidth

Function

Run the **wrr-queue bandwidth** command to configure the WRR scheduling weights for output queues.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default WRR scheduling weight ratio of output queues is **1:1:1:1:1:1:1:1**.

Syntax

wrr-queue bandwidth *weight-value-list*

no wrr-queue bandwidth

default wrr-queue bandwidth

Parameter Description

weight-value-list: WRR scheduling weights of output queues. The weight value range is from 0 to 15. The value **0** indicates that the SP scheduling policy is used.

Command Modes

Global configuration mode

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the WRR scheduling weights are configured for output queues in both global configuration mode and L2/L3 Ethernet interface configuration mode, the interface configuration prevails.

Examples

The following example sets the WRR scheduling weight ratio of global output queues to **1:1:1:2:2:2:4:8**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8
```

The following example sets the WRR scheduling weight ratio of output queues on L2 Ethernet interface GigabitEthernet 0/1 to **1:1:2:2:2:2:4:4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# wrr-queue bandwidth 1 1 2 2 2 2 4 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 wrr-queue cos-map

Function

Run the **wrr-queue cos-map** command to configure the mappings from CoS values to threshold groups.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

All CoS values are mapped to threshold group 1 by default.

Syntax

wrr-queue cos-map *threshold-id cos*&<1-8>

no wrr-queue cos-map *threshold-id*

default wrr-queue cos-map *threshold-id*

Parameter Description

threshold-id: ID of a threshold group. Two threshold groups are supported. The value range is from 1 to 2.

cos&<1-8>: CoS value. &<1-8> indicates that you can configure the mappings from 1–8 CoS values to threshold groups. The value range is from 0 to 7.

Command Modes

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

You can run the **mls qos map dscp-cos** and **wrr-queue cos-map** commands to configure DSCP-to-threshold mappings. When all the CoS values are mapped to the same threshold group, the enabled WRED on the interface is changed to RED.

Examples

The following example maps CoS values 1 and 6 to threshold group 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# wrr-queue cos-map 2 1 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 wrr-queue random-detect min-threshold

Function

Run the **wrr-queue random-detect min-threshold** command to configure the lower threshold value for WRED to discard packets.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The lower threshold value for WRED to discard packets is not configured by default.

Syntax

wrr-queue random-detect min-threshold *queue-id* [*threshold*&<1-2>]

no wrr-queue random-detect min-threshold *queue-id*

default wrr-queue random-detect min-threshold *queue-id*

Parameter Description

queue-id: ID of an interface queue. The value range is from 1 to 8.

threshold&<1-2>: Lower threshold value for WRED to discard packets, in percentage. &<1-2> indicates that you can configure 1 to 2 groups of lower threshold values. The value range is from 1 to 100.

Command Modes

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

The maximum value of the configuration range of the lower threshold is equal to the current higher threshold. When configuring a lower threshold, pay attention to the configuration of the higher threshold.

Examples

The following example sets the two groups of lower thresholds to 60 and 70 respectively for queue 1 of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# wrr-queue random-detect min-threshold 1 60
70
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 wrr-queue random-detect probability

Function

Run the **wrr-queue random-detect probability** command to configure the maximum discarding probability for WRED.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The maximum discarding probability for WRED is not configured by default.

Syntax

wrr-queue random-detect probability *queue-id probability*&<1-2>

no wrr-queue random-detect probability *queue-id*

default wrr-queue random-detect probability *queue-id*

Parameter Description

queue-id: ID of an interface queue. The value range is from 1 to 8.

probability&<1-2>: Maximum discarding probability of WRED, in percentage. &<1-2> indicates that you can configure 1 to 2 groups of maximum discarding probabilities. The value range is from 1 to 100.

Command Modes

L2 Ethernet interface configuration mode
L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the two groups of maximum discarding probabilities to 50 and 70 respectively for queue 1 of L2 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# wrr-queue random-detect probability 1 50 70
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 MMU Commands

Command	Function
mmu buffer-mode	Configure the global buffer mode.
mmu queue-guarantee	Configure a guaranteed buffer for a queue.
mmu queue-threshold	Configure a shared buffer threshold for a queue.
mmu fc-threshold	Configure a flow control threshold for a port.
mmu sample-period	Configure the monitoring data sampling period.
mmu usage-warn-limit	Configure a buffer utilization alarm threshold.
clear queue-counter	Clear the packet statistics of queues.
clear queue-buffer peaked	Clear the historical buffer utilization peak values of queues.
show queue-buffer	Display the buffer utilization information of a queue.
show queue-counter	Display the packet statistics of queues.
show mmu buffer-mode	Display the current buffer mode.

1.1 mmu buffer-mode

Function

Run the **mmu buffer-mode** command to configure the global buffer mode.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default global buffer mode is **flowctrl-enhance**.

Syntax

mmu buffer-mode { **burst-enhance** | **flowctrl-enhance** | **normal** | **qos-enhance** }

no mmu buffer-mode

default mmu buffer-mode

Parameter Description

burst-enhance: Supports burst enhancement.

flowctrl-enhance: Supports flow control enhancement.

normal: Provides relatively fair support for flow control, burst, and QoS.

qos-enhance: Supports QoS enhancement.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the buffer mode to flow control mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mmu buffer-mode flowctrl-enhance
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show mmu buffer-mode**

1.2 mmu queue-guarantee

Function

Run the **mmu queue-guarantee** command to configure a guaranteed buffer for a queue.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The guaranteed buffer for a queue is not configured by default.

Syntax

mmu queue-guarantee output unicast [*queue-id*&<1-8>] **set** *value*

no mmu queue-guarantee output unicast [*queue-id*&<1-8>]

default mmu queue-guarantee output unicast [*queue-id*&<1-8>]

Parameter Description

output: Performs buffer management on the egress queues.

unicast: Performs buffer management on the egress unicast queues.

queue-id&<1-8>: Queue ID. &<1-8> means that 1 to 8 queue IDs can be configured.

set *value*: Configures the guaranteed buffer of queue, in the unit of cell. The value range is from 1 to 50.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the parameter *queue-id*&<1-8> is not specified, all queues will be configured with the guaranteed buffer.

Examples

The following example sets the guaranteed buffer to 10 cells for unicast queue 1 on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mmu queue-guarantee output unicast 1 set 10
Hostname(config-if-GigabitEthernet 0/1)# mmu queue-guarantee output multicast 1 set 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 mmu queue-threshold

Function

Run the **mmu queue-threshold** command to configure a shared buffer threshold for a queue.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The shared buffer threshold for a queue is not configured by default.

Syntax

mmu queue-threshold output unicast [*queue-id*&<1-8>] **set** *threshold*

no mmu queue-threshold output unicast [*queue-id*&<1-8>]

default mmu queue-threshold output unicast [*queue-id*&<1-8>]

Parameter Description

output: Performs buffer management on the egress queues.

unicast: Performs buffer management on the egress unicast queues.

queue-id&<1-8>: Queue ID. &<1-8> means that 1 to 8 queue IDs can be configured.

set value: Configures the shared buffer threshold for a queue, in the unit of percentage. The value range is from 1 to 100.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the parameter *queue-id*&<1-8> is not specified, all queues will be configured with the shared buffer threshold.

Examples

The following example sets the shared buffer threshold proportion to 80% for unicast queue 1 on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mmu queue-threshold output unicast 1 set 80
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 mmu fc-threshold

Function

Run the **mmu fc-threshold** command to configure a flow control threshold for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The flow control threshold for a port is not configured by default.

Syntax

mmu fc-threshold set *threshold*

no mmu fc-threshold

default mmu fc-threshold

Parameter Description

set *threshold*: Configures a flow control threshold for a port, in percentage. The value range is from 1 to 100.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The configuration takes effect only when flow control/priority-based flow control (PFC) is enabled on the port.

Examples

The following example sets the flow control threshold to 20% for interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mmu fc-threshold set 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 mmu sample-period

Function

Run the **mmu sample-period** command to configure the monitoring data sampling period.

Run the **no mmu sample-period** command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The monitoring data sampling period is not configured by default.

Syntax

mmu sample-period set *period*

no mmu sample-period

default mmu sample-period

Parameter Description

set *period*: Configures the sampling period, in seconds. The value range is from 5 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the monitoring data sampling period to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mmu sample-period set 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 mmu usage-warn-limit

Function

Run the **mmu usage-warn-limit** command to configure a buffer utilization alarm threshold.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The buffer utilization alarm threshold is not configured by default.

Syntax

(Global configuration mode)

mmu usage-warn-limit set *threshold*

no mmu usage-warn-limit

default mmu usage-warn-limit

(Interface configuration mode)

mmu usage-warn-limit unicast [*queue-id*&<1-8>] **set** *threshold*

no mmu usage-warn-limit unicast [*queue-id*&<1-8>]]

default mmu usage-warn-limit unicast [*queue-id*&<1-8>]]

Parameter Description

unicast: Configures the buffer utilization alarm threshold for egress unicast queues.

queue-id&<1-8>: Queue ID. &<1-8> means that 1 to 8 queue IDs can be configured.

set value: Configures the buffer utilization alarm threshold for a queue, in the unit of percentage. The value range is from 1 to 100.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

If the parameter *queue-id*&<1-8> is not specified, all queues will be configured with the buffer utilization alarm threshold.

The buffer utilization alarm threshold of port groups or slices takes effect for all the port groups or slices. To prevent frequent log refreshing, the alarm logs of the same port group, slice, port, or queue are printed once in 30s at most. The maximum printing interval depends on the configured sampling period.

Examples

The following example sets the buffer utilization alarm threshold to 80% for slices.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mmu usage-warn-limit set 80
```

The following example sets the buffer utilization alarm threshold to 70% for unicast queues 6 and 7 on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mmu usage-warn-limit unicast 6 7 set 70
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 clear queue-counter

Function

Run the **clear queue-counter** command to clear the packet statistics of queues.

Syntax

clear queue-counter [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Clears the packet statistics of queues of a specified interface type and number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the packet statistics of all queues.

```
Hostname> enable
Hostname# clear queue-counter
```

The following example clears the packet statistics of queues on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear queue-counter interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.8 clear queue-buffer peaked

Function

Run the **clear queue-buffer peaked** command to clear the historical buffer utilization peak values of queues.

Syntax

clear [**mmu**] **queue-buffer peaked** [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Clears the historical buffer utilization peak values of queues of a specified interface type and number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the historical buffer utilization peak values of all the queues.

```
Hostname> enable
Hostname# clear queue-buffer peaked
```

The following example clears the historical buffer utilization peak values of the queues on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear queue-buffer peaked interface GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show queue-buffer

Function

Run the **show queue-buffer** command to display the buffer utilization information of a queue.

Syntax

show queue-buffer [**interface** [*interface-type interface-number*]]

Parameter Description

interface: Displays the buffer utilization information of queues on all the interfaces.

interface-type interface-number: Interface type and interface number. After this parameter is specified, the buffer utilization information of queues of a specified interface type and number are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the buffer utilization information of queues on interface GigabitEthernet 0/1. The output information is displayed based on egress queues.

```
Hostname> enable
Hostname# show queue-buffer interface gigabitethernet 0/1
Dev/slot   Port-group   Total-shared(%)   Guarantee-used(%)   Share-used(%)
Available(%)   Warn-limit(%)
1/-       1          84.7348         0.0000            0.0000         100.0000
NA

Interface GigabitEthernet 0/1:
Type       Queue   Admin-shared(%)   Total-used(%)   Available(%)   Warn-limit(%)
Peak-usage(%)   Peak-time
Unicast    1      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    2      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    3      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    4      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    5      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    6      (default)        0.0000         67.8248       NA            0.0000
NA
Unicast    7      (default)        0.0000         67.8248       NA            0.0000
NA
```

```
Unicast    8      (default)        0.0000         67.8248       NA            0.0000
NA
Multicast  1      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  2      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  3      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  4      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  5      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  6      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  7      (default)        0.0000         9.4521        NA            0.0000
NA
Multicast  8      (default)        0.0000         9.4521        NA            0.0000
NA
```

Table 1-1 Output Fields of the show queue-buffer interface Command, Displayed Based on Egress Queues

Field	Description
Dev/Slot	Device/Slot ID. ● For a box-type device, the value is displayed in the format of device ID/-.
Port-Group	Port group ID.
Total-shared	Percentage of the buffer that can be shared by the port group relative to the total buffer resource of the port group.
Guarantee-used	Percentage of the guaranteed buffer that has been used by the port group relative to the total buffer resource of the port group.
Share-used	Percentage of the shared buffer that has been used by the port group relative to the total buffer resource of the port group.
Available	Percentage of the remaining buffer that can be shared by the port group relative to the total buffer resource of the port group, or percentage of buffer currently available for a queue. Since multiple queues are preempting the shared buffer, the size of the buffer that can be requested by a queue is smaller than or equal to the **Available** value.
Warn-limit	Buffer utilization alarm threshold of the specified port group or a queue.

Field	Description
Type	Queue type: ● Unicast: Indicates a unicast queue. ● Multicast: Indicates a multicast queue.
Queue	Queue ID.
Total-used	Percentage of the buffer used in the queue, including the guaranteed buffer and shared buffer, relative to the total buffer resource of the port group.
Peak-usage	Historical buffer utilization peak value, in percentage.
Peak-time	Time corresponding to the utilization peak value.
NA	No data.

The following example displays the buffer usage information of all the ports, summarizing the queue statistics of all the ports.

```
Hostname> enable
Hostname# show queue-buffer interface
Dev/slot   Port-group   Total-shared(%)   Guarantee-used(%)   Share-used(%)
Available(%)   Warn-limit(%)
1/-       1           84.7348          0.0000            0.0000         100.0000
NA

Interface    Total-used(%)        available(%)
Hu0/1        0.0000              67.8248
Hu0/2        0.0000              67.8248
Hu0/3        0.0000              67.8248
Hu0/4        0.0000              67.8248
Hu0/5        0.0000              67.8248
Hu0/6        0.0000              67.8248
Hu0/7        0.0000              67.8248
Hu0/8        0.0000              67.8248
Hu0/9        0.0000              67.8248
…
```

Table 1-2 Output Fields of the show queue-buffer interface Command, Displayed Based on Ports

Field	Description
Dev/Slot	Device/Slot ID. ● For the box-type device, the display format is device ID/-.

Field	Description
Port-Group	Port group ID.
Total-shared	Percentage of the buffer that can be shared by the port group relative to the total buffer resource of the port group.
Guarantee-used	Percentage of the guaranteed buffer that has been used by the port group relative to the total buffer resource of the port group.
Share-used	Percentage of the shared buffer that has been used by the port group relative to the total buffer resource of the port group.
Available	Percentage of the remaining buffer that can be shared by the port group relative to the total buffer resource of the port group.
Warn-limit	Buffer utilization alarm threshold of the specified port group.
Interface	Interface.
Total-used	Percentage of the total buffer that has been used by all queues of the port, relative to the total buffer resource of the port group.
available	Percentage of the maximum available buffer in the queues of the port, relative to the total buffer resource of the port group.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show queue-counter

Function

Run the **show queue-counter** command to display the packet statistics of queues.

Syntax

show queue-counter [**interface** [*interface-type interface-number*]]

Parameter Description

interface: Displays the packet statistics of queues on all the interfaces.

interface-type interface-number: Interface type and interface number. After this parameter is specified, the packet statistics of queues of a specified interface type and number are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the packet statistics of queues on interface GigabitEthernet 0/1, displayed based on egress queues.

```
Hostname> enable
Hostname# show queue-counter interface gigabitethernet 0/1
  Unicast
  Queue    Transmitted Bytes        Dropped Bytes    Transmit Rate(bps)    Loss Rate(%)
Loss Rate Peak(%)         Loss Peak Time
     1                   0                   0                   0             0
0                   NA
     2                   0                   0                   0             0
0                   NA
     3                   0                   0                   0             0
0                   NA
     4                   0                   0                   0             0
0                   NA
     5                   0                   0                   0             0
0                   NA
     6                   0                   0                   0             0
0                   NA
     7                   0                   0                   0             0
0                   NA
     8                   0                   0                   0             0
0                   NA
  Queue   Transmitted Packets      Dropped Packets    Transmit Rate(pps)    Loss Rate(%)
Loss Rate Peak(%)         Loss Peak Time
```

```
     1                  0                  0                  0             0
0                   NA
     2                  0                  0                  0             0
0                   NA
     3                  0                  0                  0             0
0                   NA
     4                  0                  0                  0             0
0                   NA
     5                  0                  0                  0             0
0                   NA
     6                  0                  0                  0             0
0                   NA
     7                  0                  0                  0             0
0                   NA
     8                  0                  0                  0             0
0                   NA
  Multicast
  Queue    Transmitted Bytes        Dropped Bytes    Transmit Rate(bps)    Loss Rate(%)
Loss Rate Peak(%)         Loss Peak Time
     1                  0                  0                  0             0
0                   NA
     2                  0                  0                  0             0
0                   NA
     3                  0                  0                  0             0
0                   NA
     4                  0                  0                  0             0
0                   NA
     5                  0                  0                  0             0
0                   NA
     6                  0                  0                  0             0
0                   NA
     7                  0                  0                  0             0
0                   NA
     8                  0                  0                  0             0
0                   NA
  Queue   Transmitted Packets      Dropped Packets    Transmit Rate(pps)    Loss Rate(%)
Loss Rate Peak(%)         Loss Peak Time
     1                  0                  0                  0             0
0                   NA
     2                  0                  0                  0             0
0                   NA
     3                  0                  0                  0             0
0                   NA
```

```
      4                    0                    0                    0                    0
0                     NA
      5                    0                    0                    0                    0
0                     NA
      6                    0                    0                    0                    0
0                     NA
      7                    0                    0                    0                    0
0                     NA
```

Table 1-3 Output Fields of the show queue-counter interface Command, Displayed Based on Egress Queues

Field	Description
Unicast	Unicast queue.
Multicast	Multicast queue.
Queue	Queue ID.
Transmitted Bytes	Number of bytes that have been forwarded by the specified queue.
Dropped Bytes	Number of bytes that have been dropped by the specified queue.
Transmitted Packets	Number of packets that have been forwarded by the specified queue.
Dropped Packets	Number of packets that have been dropped by the specified queue.
Transmit Rate(bps)	Average forwarding rate (bps) of the specified queue in a period of time (longer than or equal to the sampling period). The rate is calculated with the interframe gap included, and the value has a certain margin of calculation error.
Transmit Rate(pps)	Average forwarding rate (packets per second) of the specified queue in a period of time (longer than or equal to the sampling cycle). The value has a certain margin of calculation error.
Loss Rate(%)	Loss rate of bytes or packets of the specified queue. ● Byte loss rate = Number of lost bytes/(Number of lost bytes + Number of forwarded bytes). ● Packet loss rate = Number of lost packets/(Number of lost packets + Number of forwarded packets).
Loss Rate Peak(%)	Historical peak value of the loss rate.
Loss Peak Time	Time point, at which the historical peak value of the loss rate occurs.
NA	No data.

The following example displays the packet statistics of all the ports, summarizing the queue statistics of all the ports.

```
Hostname> enable
Hostname# show queue-counter interface
Interface    Transmitted Bytes    Dropped Bytes       Transmit Rate(bps)    Loss
Rate(%)
Hu0/1        0                    0                   0                     0.000
Hu0/2        0                    0                   0                     0.000
Hu0/3        0                    0                   0                     0.000
Hu0/4        0                    0                   0                     0.000
Hu0/5        0                    0                   0                     0.000
Hu0/6        0                    0                   0                     0.000
Hu0/7        0                    0                   0                     0.000
Hu0/8        0                    0                   0                     0.000
Hu0/9        0                    0                   0                     0.000
Hu0/10       0                    0                   0                     0.000
Hu0/11       0                    0                   0                     0.000
Hu0/12       0                    0                   0                     0.000
Hu0/13       0                    0                   0                     0.000
Hu0/14       0                    0                   0                     0.000
Hu0/15       0                    0                   0                     0.000
Hu0/16       0                    0                   0                     0.000
Hu0/17       0                    0                   0                     0.000
Hu0/18       0                    0                   0                     0.000
…
Interface    Transmitted Packets   Dropped Packets      Transmit Rate(pps)    Loss
Rate(%)
Hu0/1        0                    0                   0                     0.000
Hu0/2        0                    0                   0                     0.000
Hu0/3        0                    0                   0                     0.000
Hu0/4        0                    0                   0                     0.000
Hu0/5        0                    0                   0                     0.000
Hu0/6        0                    0                   0                     0.000
Hu0/7        0                    0                   0                     0.000
Hu0/8        0                    0                   0                     0.000
Hu0/9        0                    0                   0                     0.000
Hu0/10       0                    0                   0                     0.000
Hu0/11       0                    0                   0                     0.000
Hu0/12       0                    0                   0                     0.000
Hu0/13       0                    0                   0                     0.000
Hu0/14       0                    0                   0                     0.000
Hu0/15       0                    0                   0                     0.000
Hu0/16       0                    0                   0                     0.000
Hu0/17       0                    0                   0                     0.000
Hu0/18       0                    0                   0                     0.000
```

...

Table 1-4 Output Fields of the show queue-counter multicast Command, Displayed Based on Ports

Field	Description
Interface	Interface.
Transmitted Bytes	Total number of bytes that have been forwarded by all the queues of the port.
Dropped Bytes	Total number of bytes that have been dropped by all the queues of the port.
Transmitted Packets	Total number of packets that have been forwarded by all the queues of the port.
Dropped Packets	Total number of packets that have been dropped by all the queues of the port.
Transmit Rate(bps)	Average forwarding rate (bps) of all the queues on the port in a period of time (longer than or equal to the sampling period). The rate is calculated with the interframe gap included and the value has a certain margin of calculation error.
Transmit Rate(pps)	Average forwarding rate (packets per second) of all the queues on the port in a period of time (longer than or equal to the sampling period). The value has a certain margin of calculation error.
Loss Rate(%)	Total loss rate of bytes or packets of all the queues on the port. ● Byte loss rate = Number of lost bytes/(Number of lost bytes + Number of forwarded bytes). ● Packet loss rate = Number of lost packets/(Number of lost packets + Number of forwarded packets).

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show mmu buffer-mode

Function

Run the **show mmu buffer-mode** command to display the current buffer mode.

Syntax

show mmu buffer-mode

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the current buffer mode.

```
Hostname> enable
Hostname# show mmu buffer-mode
mmu buffer-mode: flowctrl-enhance
```

Table 1-5 Output Fields of the show mmu buffer-mode Command

Field	Description
mmu buffer-mode	Global buffer mode type

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

Security Commands

1 AAA Commands

Command	Function
aaa accounting commands	Configure a command accounting method list.
aaa accounting exec	Configure an EXEC accounting method list.
aaa accounting network	Configure a network accounting method list.
aaa accounting start-fail	Configure the user online/offline status after an accounting start failure.
aaa accounting update	Enable accounting update.
aaa accounting update periodic	Configure an accounting update interval.
aaa authentication dot1x	Configure an IEEE 802.1X authentication method list.
aaa authentication ftp	Configure a method list for File Transfer Protocol (FTP) authentication.
aaa authentication enable default	Configure the default method list for Enable authentication.
aaa authentication general	Configure a general authentication method list.
aaa authentication login	Configure a login authentication method list.
aaa authentication web-auth	Configure a 2nd-generation Web authentication method list.

aaa authorization config-commands	Enable command authorization in configuration modes (including global configuration mode and their submodes).
aaa authorization console	Enable command authorization for users who log in through the console.
aaa authorization exec	Configure an EXEC authorization method list.
aaa authorization network	Configure a network authorization method list.
aaa command-author cache	Enable the function of caching command authorization results.
aaa domain	Create a domain and enter the domain configuration mode.
aaa domain enable	Enable the domain-based AAA services.
aaa heartbeat enable	Enable AAA heartbeat service.
aaa local authentication attempts	Configure the maximum number of consecutive failed login attempts.
aaa local authentication lockout-time	Configure the account lockout duration after the number of consecutive failed login attempts of a user reaches the configured value.
aaa local user allow public account	Enable the function of allowing multiple clients to share a Web-authenticated local account.
aaa log enable	Enable AAA authentication logging.
aaa log rate-limit	Configure the rate of AAA user authentication success logging.

aaa new-model	Enable AAA security services.
aaa user-role default	Configure the default role for AAA authorized users.
access-limit	Configure a limit on the number of users supported in a domain.
accounting network	Configure a network accounting method list for an AAA domain.
accounting commands	Configure a command accounting method list for an AAA domain.
accounting exec	Configure an EXEC accounting method list for an AAA domain.
authentication dot1x	Configure an IEEE 802.1X authentication method list for an AAA domain.
authentication login	Configure a login authentication method list for an AAA domain.
authentication enable	Configure an Enable authentication method list for an AAA domain.
authorization network	Configure a network authorization method list for an AAA domain.
authorization commands	Configure a command authorization method list for an AAA domain.
authorization exec	Configure an EXEC authorization method list for an AAA domain.
clear aaa local user lockout	Clear the list of locked users.

show aaa accounting update	Display accounting update information.
show aaa domain	Display information about a configured domain.
show aaa lockout	Display lockout parameter configuration in the current login authentication.
show aaa group	Display all AAA server groups.
show aaa method-list	Display all AAA method lists.
show aaa user	Display information about an AAA user.
state	Configure the status of a domain.
username-format	Configure whether usernames carry domain name information during interaction between the device and the server.

Note

- Before configuring authentication, authorization and accounting (AAA) commands, run the **aaa new-model** command to enable AAA security services.
- If there are multiple methods in the authentication, authorization, or accounting method list, the methods are applied based on their sequence in the method list. The device switches to the next method only when a method fails to respond.

1.1 aaa accounting commands

Function

Run the **aaa accounting commands** command to configure a command accounting method list.

Run the **no** form of this command to remove this configuration.

No command accounting method list is configured by default.

Syntax

aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method*&<1-4>

no aaa accounting commands *level* { **default** | *list-name* }

Parameter Description

level: Level of commands, for which accounting needs to be performed. Information will be recorded when a command of the configured level is executed. The value range is from 0 to 15.

default: Defines the default command accounting method list.

list-name: Name of a command accounting method list. The value is a string of 1 to 63 characters.

method&<1-4>: Command accounting method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for accounting. Only Terminal Access Controller Access-Control System Plus (TACACS+) server groups are supported. You can enter this type parameter 0–4 times in this command.

- **group tacacs+**: Uses all TACACS+ servers for accounting. You can enter this type parameter only once in this command.
- **none**: Indicates no accounting. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A configured command accounting method must be applied to a line that needs command accounting so that the method takes effect.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

If the role-based access control (RBAC) function is enabled, this command is unavailable.

Command accounting can be enabled for a user only after the user passes login authentication. If a user is not authenticated or is exempt from authentication during login, command accounting is not performed. After command accounting is enabled, the device records information about the commands of a specified level run by a user each time and sends it to the security server for accounting and user activity management.

Examples

The following example configures the default command accounting method, in which all TACACS+ servers are used to perform accounting on commands of level 15 run by users who log in to the network access server (NAS).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed.
```

When the configured group type does not support the accounting type, the following notification will be displayed:

```
The accounting does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **accounting commands** (basic configuration/line)

1.2 aaa accounting exec

Function

Run the **aaa accounting exec** command to configure an EXEC accounting method list.

Run the **no** form of this command to remove this configuration.

No EXEC accounting method list is configured by default.

Syntax

aaa accounting exec { **default** | *list-name* } **start-stop** *method*&<1-4>

no aaa accounting exec { **default** | *list-name* }

Parameter Description

default: Defines the default EXEC accounting method list.

list-name: Name of an EXEC accounting method list. The value is a string of 1 to 63 characters.

method&<1-4>: EXEC accounting method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for accounting. Only the Remote Authentication Dial-In User Service (RADIUS) and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for accounting. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for accounting. You can enter this type parameter only once in this command.
- **none**: Indicates no accounting. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After accounting is enabled, the NAS sends an accounting start message to the security server when a user logs in to the NAS CLI, and sends an accounting stop message to the security server when the user logs out. If the NAS does not send an accounting start message when a user logs in, it will not send an accounting stop message when the user logs out.

A configured EXEC accounting method must be applied to a line that needs EXEC accounting. Otherwise, the method does not take effect.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

EXEC accounting can be enabled for a user only after the user passes login authentication. If a user is not authenticated during login or the **none** authentication method is adopted, EXEC accounting will not be performed.

Examples

The following example configures the default EXEC accounting method list, in which all RADIUS server groups are used to perform accounting on access activities of users who log in to the NAS, and send accounting packets at user login and logout.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa accounting exec default start-stop group radius
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the accounting type, the following notification will be displayed:

```
The accounting does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **accounting exec** (basic configuration/line)

1.3 aaa accounting network

Function

Run the **aaa accounting network** command to configure a network accounting method list.

Run the **no** form of this command to remove this configuration.

No network accounting method list is configured by default.

Syntax

aaa accounting network { **default** | *list-name* } **start-stop** *method*&<1-4>

no aaa accounting network { **default** | *list-name* }

Parameter Description

default: Defines the default network accounting method list.

list-name: Name of a network accounting method list. The value is a string of 1 to 63 characters.

method&<1-4>: Network accounting method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for accounting. Only the RADIUS and TACACS+ server groups are supported. You can enter this parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for accounting. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for accounting. You can enter this type parameter only once in this command.
- **none**: Indicates no accounting. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Accounting packets are sent when a user starts and ends the access. The accounting start packet indicates that a user is allowed to access the network regardless of whether accounting is successfully enabled.

Examples

The following example configures the default network accounting method list, in which all RADIUS servers are used to perform accounting on network service requests of users, and send accounting packets when the user access activity starts and ends.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa accounting network default start-stop group radius
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the accounting type, the following notification will be displayed:

```
The accounting does not support this type of group
```

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Common Errors

N/A

Related Commands

- **dot1x accounting** (IEEE 802.1X)

1.4 aaa accounting start-fail

Function

Run the **aaa accounting start-fail** command to configure the user online/offline status after an accounting start failure.

Run the **no** form of this command to restore the default configuration.

The user online/offline status after an accounting start failure is not configured by default.

Syntax

aaa accounting start-fail { **offline** | **online** }

no aaa accounting start-fail

Parameter Description

offline: Sets the accounting start failure policy to offline.

online: Sets the accounting start failure policy to online.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a policy for user accounting start failures and specify the user online/offline status after the user accounting start fails.

Examples

The following example sets the user status after an accounting start failure to offline.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa accounting start-fail offline
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 aaa accounting update

Function

Run the **aaa accounting update** command to enable accounting update.

Run the **no** form of this command to disable this feature.

Accounting update is disabled by default.

Syntax

aaa accounting update

no aaa accounting update

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can help improve the accounting accuracy. You are advised to configure it.

Examples

The following example enables accounting update.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 aaa accounting update periodic

Function

Run the **aaa accounting update periodic** command to configure an accounting update interval.

Run the **no** form of this command to restore the default configuration.

The default accounting update interval is **5** minutes.

Syntax

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter Description

interval: Accounting update interval, in minutes. The value range is from 1 to 525600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

It is recommended that the accounting update interval not be configured unless otherwise specified.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the accounting update interval to **1** minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update
Hostname(config)# aaa accounting update periodic 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa accounting update**

1.7 aaa authentication dot1x

Function

Run the **aaa authentication dot1x** command to configure an IEEE 802.1X authentication method list.

Run the **no** form of this command to remove this configuration.

No IEEE 802.1X authentication method list is configured by default.

Syntax

aaa authentication dot1x { **default** | *list-name* } *method*&<1-4>

no aaa authentication dot1x { **default** | *list-name* }

Parameter Description

default: Defines the default IEEE 802.1X authentication method list.

list-name: Name of an IEEE 802.1X authentication method list. The value is a string of 1 to 63 characters.

method&<1-4>: IEEE 802.1X authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authentication. Only RADIUS server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authentication. You can enter this type parameter only once in this command.
- **local**: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the IEEE 802.1X authentication service is enabled on the device, IEEE 802.1X authentication must be performed when a user accesses the device network. You can configure this command to provide a method list for IEEE 802.1X authentication. An IEEE 802.1X authentication method needs to be applied so that the method takes effect.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures an IEEE 802.1X authentication method list named **rds_d1x**, in which a RADIUS server is used for authentication first, and the local user database is used for authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authentication dot1x rds_d1x group radius local
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dot1x authentication** (IEEE 802.1X)

1.8 aaa authentication ftp

Function

Run the **aaa authentication ftp** command to configure a method list for File Transfer Protocol (FTP) authentication.

Run the **no** form of this command to remove this configuration.

No FTP authentication method list is configured by default.

Syntax

aaa authentication ftp { **default** | *list-name* } *method*&<1-4>

no aaa authentication ftp { **default** | *list-name* }

Parameter Description

default: Defines the default FTP authentication method list.

list-name: Name of an FTP authentication method list. The value is a string of 1 to 63 characters.

method&<1-4>: FTP authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authentication. Only the RADIUS and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authentication. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for authentication. You can enter this type parameter only once in this command.
- **local**: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.

- **none**: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the AAA FTP security service is enabled on the device, FTP authentication must be performed through AAA when an FTP user accesses the device.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures an FTP authentication method list named **rds_ftp**, in which a RADIUS server is used for authentication first, and the local user database is used for authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authentication ftp rds_ftp group radius local
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server authentication** (network management and monitoring/FTP server)

1.9 aaa authentication enable default

Function

Run the **aaa authentication enable default** command to configure the default method list for Enable authentication.

Run the **no** form of this command to remove this configuration.

No default method list for Enable authentication is configured by default.

Syntax

aaa authentication enable default *method*&<1-4>

no aaa authentication enable default

Parameter Description

method&<1-4>: Configured Enable authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **enable**: Uses the Enable server for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **group** *group-name*: Uses a server group for authentication. Only the RADIUS and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authentication. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for authentication. You can enter this type parameter only once in this command.

- **local**: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the AAA Enable authentication service is enabled on the device, users must perform Enable authentication through AAA.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures the default method list for Enable authentication, in which a RADIUS server is used for authentication first, and the local user database is used for authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authentication enable default group radius local
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 aaa authentication general

Function

Run the **aaa authentication general** command to configure a general authentication method list.

Run the **no** form of this command to remove this configuration.

No general authentication method list is configured by default.

Syntax

aaa authentication general { **default** | *list-name* } *method*&<1-4>

no aaa authentication general { **default** | *list-name* }

Parameter Description

default: Defines the default general authentication method list.

list-name: Name of a general authentication method list. The value is a string of 1 to 63 characters.

method&<1-4>: General authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authentication. Only RADIUS server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authentication. You can enter this type parameter only once in this command.

- **local**: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If both IEEE 802.1X authentication and Web authentication are used on the device and the configured authentication methods are the same, you can configure a general authentication method for them together. If both an IEEE 802.1X authentication method (or Web authentication method) and a general authentication method are configured, the IEEE 802.1X authentication method (or Web authentication method) is preferred.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures a general authentication method list, in which a RADIUS server is used for authentication first, and the local user database is used for authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authentication general default group radius local
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 aaa authentication login

Function

Run the **aaa authentication login** command to configure a login authentication method list.

Run the **no** form of this command to remove this configuration.

No login authentication method list is configured by default.

Syntax

aaa authentication login { **default** | *list-name* } *method*&<1-4>

no aaa authentication login { **default** | *list-name* }

Parameter Description

default: Defines the default login authentication method list.

list-name: Name of a login authentication method list. The value is a string of 1 to 63 characters.

method&<1-4>: Login authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authentication. Only the RADIUS and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authentication. You can enter this type parameter only once in

this command.

- **group tacacs+**: Uses all TACACS+ servers for authentication. You can enter this type parameter only once in this command.
- **local**: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the AAA login authentication security service is enabled on the device, users must perform login authentication through AAA upon login.

A configured login authentication method must be applied to a line that needs login authentication. Otherwise, the method does not take effect.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures a login authentication method list named **list-1**, in which a RADIUS server is used for authentication first, and the local user database is used for authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authentication login list-1 group radius local
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **login authentication** (basic configuration/basic management)

1.12 aaa authentication web-auth

Function

Run the **aaa authentication web-auth** command to configure a 2nd-generation Web authentication method list.

Run the **no** form of this command to remove this configuration.

No 2nd-generation Web authentication method list is configured by default.

Syntax

aaa authentication web-auth { **default** | *list-name* } *method*&<1-4>

no aaa authentication web-auth { **default** | *list-name* }

Parameter Description

default: Defines the default 2nd-generation Web authentication method list.

list-name: Name of a 2nd-generation Web authentication method list. A maximum of four methods can be configured in a method list. The value is a string of 1 to 63 characters.

method&<1-4>: 2nd-generation Web authentication method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

group *group-name*: Uses a server group for authentication. Only RADIUS server groups are supported. You can enter this type parameter 0–4 times in this command.

group radius: Uses all RADIUS servers for authentication. You can enter this type parameter only once in this command.

local: Uses the local user database for authentication. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.

none: Indicates no authentication. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the 2nd-generation Web authentication service is enabled on the device, 2nd-generation Web authentication must be performed when a user accesses the device.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures a 2nd-generation Web authentication method list named **rds_web**, in which a RADIUS server is used for authentication first, and user packets are allowed to pass through and users pass authentication if no response is received from the RADIUS server within a period of time.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# aaa authentication web-auth rds_web group radius none
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authentication type, the following notification will be displayed:

```
The authentication does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **Authentication** (Web authentication)

1.13 aaa authorization config-commands

Function

Run the **aaa authorization config-commands** command to enable command authorization in configuration modes (including global configuration mode and their submodes).

Run the **no** form of this command to disable this feature.

Command authorization in configuration modes is disabled by default.

Syntax

aaa authorization config-commands

no aaa authorization config-commands

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If you need to grant authorization to commands only in non-configuration modes (such as privileged EXEC mode), use the **no** form of this command to disable command authorization in configuration modes, that is, commands in configuration modes and their submodes can be executed without authorization.

Examples

The following example enables command authorization in configuration modes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authorization config-commands
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 aaa authorization console

Function

Run the **aaa authorization console** command to enable command authorization for users who log in through the console.

Run the **no** form of this command to disable this feature.

Command authorization is disabled for users who log in through the console by default.

Syntax

aaa authorization console

no aaa authorization console

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The device differentiates users who log in through the console from those who log in through other terminals. This command is used to enable command authorization for users who log in through the console.

If command authorization is disabled for users who log in through the console, the command authorization method list that has been applied to the console line is invalidated.

Examples

The following example enables command authorization for users who log in through the console.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# aaa authorization console
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 aaa authorization exec

Function

Run the **aaa authorization exec** command to configure an EXEC authorization method list.

Run the **no** form of this command to remove this configuration.

No EXEC authorization method list is configured by default.

Syntax

aaa authorization exec { **default** | *list-name* } *method*&<1-4>

no aaa authorization exec { **default** | *list-name* }

Parameter Description

default: Defines the default EXEC authorization method list.

list-name: Name of an EXEC authorization method list. A maximum of four methods can be configured in a method list. The value is a string of 1 to 63 characters.

method&<1-4>: EXEC authorization method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authorization, Only the RADIUS and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authorization. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for authorization. You can enter this type parameter only once in this command.
- **local**: Uses the local user database for authorization. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authorization. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The device allows granting CLI permissions (levels 0 to 15) to users who log in to the CLI. EXEC authorization is performed only on users who pass login authentication. If a user fails in EXEC authorization, the user cannot open the CLI.

A configured EXEC authorization method must be applied to a line that needs EXEC authorization. Otherwise, the method does not take effect.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures the default EXEC authorization method list, in which RADIUS servers are used for EXEC authorization.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authorization exec default group radius
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authorization type, the following notification will be displayed:

```
The authorization does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **authorization commands** (basic configuration/line)

1.16 aaa authorization network

Function

Run the **aaa authorization network** command to configure a network authorization method list.

Run the **no** form of this command to remove this configuration.

No network authorization method list is configured by default.

Syntax

aaa authorization network { **default** | *list-name* } *method*&<1-4>

no aaa authorization network { **default** | *list-name* }

Parameter Description

default: Defines the default network authorization method list.

list-name: Name of a network authorization method list. A maximum of four methods can be configured in a method list. The value is a string of 1 to 63 characters.

method&<1-4>: Network authorization method. &<1-4> indicates that 1–4 methods can be configured in a list. The optional types of *method* are as follows:

- **group** *group-name*: Uses a server group for authorization. Only the RADIUS and TACACS+ server groups are supported. You can enter this type parameter 0–4 times in this command.
- **group radius**: Uses all RADIUS servers for authorization. You can enter this type parameter only once in this command.
- **group tacacs+**: Uses all TACACS+ servers for authorization. You can enter this type parameter only once in this command.
- **local**: Uses the local user database for authorization. You can enter this type parameter only once in this command. After entering this parameter, you can also enter other type parameters.
- **none**: Indicates no authorization. You can enter this type parameter only once in this command. After entering this parameter, you cannot enter other types.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The device supports authorization on all network-related services. After authorization is configured, all authenticated users or interfaces are authorized automatically.

A RADIUS or TACACS+ server completes authorization of authenticated users by returning a series of attributes. Therefore, network authorization is based on authentication. Only authenticated users can gain network authorization.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example configures the default network authorization method list, in which RADIUS servers are used to provide authorization for network service requirements.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authorization network default group radius
```

Notifications

When the specified group is not defined on the device, the following notification will be displayed:

```
%Group XXX is not existed
```

When the configured group type does not support the authorization type, the following notification will be displayed:

```
The authorization does not support this type of group
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 aaa command-author cache

Function

Run the **aaa command-author cache** command to enable the function of caching command authorization results.

Run the **no** form of this command to disable this feature.

The function of caching command authorization results is disabled by default.

Syntax

aaa command-author cache

no aaa command-author cache

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The device can locally cache command authorization results returned by an AAA server. Subsequent authorization of commands with the level same as the cached authorized commands are performed based on the locally cached results.

Cached command authorization results are valid only to the current session and commands of the current level.

Examples

The following example enables the function of caching command authorization results.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa command-author cache
```

Notifications

N/A

Common Errors

N/A

Platform Description

Switching platform

Related Commands

N/A

1.18 aaa domain

Function

Run the **aaa domain** command to create a domain and enter the domain configuration mode.

Run the **no** form of this command to remove this configuration.

No domain is configured by default.

Syntax

aaa domain { **default** | *domain-name* }

no aaa domain { **default** | *domain-name* }

Parameter Description

default: Enters the configuration mode of the default domain.

domain-name: Name of a domain. After this parameter is configured, the system enters the configuration mode of the domain.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Before running this command, run the **aaa domain enable** command to enable the domain-based AAA services first.

After the domain-based AAA services are enabled, if information of a user does not carry domain information, the user belongs to the default domain **default**.

domain-name indicates the domain name. If information of a user carries the domain name, the method list associated with this domain is used. The system supports a maximum of 32 domains.

Examples

The following example enters the configuration mode of a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**

1.19 aaa domain enable

Function

Run the **aaa domain enable** command to enable the domain-based AAA services.

Run the **no** form of this command to disable this feature.

The domain-based AAA services are disabled by default.

Syntax

aaa domain enable

no aaa domain enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the domain-named AAA services.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 aaa heartbeat enable

Function

Run the **aaa heartbeat enable** command to enable AAA heartbeat service.

Run the **no** command to disable this feature.

Run the **default** command to restore the default configuration.

AAA heartbeat service is enabled by default.

Syntax

aaa heartbeat enable
no aaa heartbeat enable
default aaa heartbeat enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Enable this feature to solve the problem that the AAA function is unavailable due to abnormal internal disconnection under special circumstances.

The heartbeat message sending interval is 60 seconds, which has little impact on performance. It is recommended to keep it enabled.

Examples

The following example disable the AAA heartbeat service.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no aaa heartbeat enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 aaa local authentication attempts

Function

Run the **aaa local authentication attempts** command to configure the maximum number of consecutive failed login attempts.

Run the **no** command to restore the default configuration.

The default maximum number of consecutive failed login attempts is **3**.

Syntax

aaa local authentication attempts *max-attempts*

no aaa local authentication attempts

Parameter Description

max-attempts: Maximum number of consecutive failed login attempts. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of consecutive failed login attempts to **6**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa local authentication attempts 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show aaa lockout**

1.22 aaa local authentication lockout-time

Function

Run the **aaa local authentication lockout-time** command to configure the account lockout duration after the number of consecutive failed login attempts of a user reaches the configured value.

Run the **no** form of this command to restore the default configuration.

An account is locked for 15 minutes after the number of consecutive failed login attempts using the account reaches the configured value by default.

Syntax

aaa local authentication lockout-time *lockout-time*

no aaa local authentication lockout-time

Parameter Description

lockout-time: Account lockout duration, in minutes. The value range is from 1 to 43200.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the account lockout duration after the number of consecutive failed login attempts reaches the configured value to **5** minutes.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# aaa local authentication lockout-time 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa heartbeat enable**
- **Function**

Run the **aaa heartbeat enable** command to enable AAA heartbeat service.

Run the **no** command to disable this feature.

Run the **default** command to restore the default configuration.

AAA heartbeat service is enabled by default.

Syntax

aaa heartbeat enable
no aaa heartbeat enable
default aaa heartbeat enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Enable this feature to solve the problem that the AAA function is unavailable due to abnormal internal disconnection under special circumstances.

The heartbeat message sending interval is 60 seconds, which has little impact on performance. It is recommended to keep it enabled.

Examples

The following example disable the AAA heartbeat service.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no aaa heartbeat enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

- aaa local authentication attempts

1.23 aaa local user allow public account

Function

Run the **aaa local user allow public account** command to enable the function of allowing multiple clients to share a Web-authenticated local account.

Run the **no** form of this command to restore the default configuration.

The function of allowing multiple clients to share a Web-authenticated local account is disabled by default.

Syntax

aaa local user allow public account

no aaa local user allow public account

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of allowing multiple clients to share a Web-authenticated local account.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa local user allow public account
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 aaa log enable

Function

Run the **aaa log enable** command to enable AAA authentication logging.

Run the **no** form of this command to disable this feature.

AAA authentication logging is enabled by default.

Syntax

aaa log enable

no aaa log enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a large number of users go online, considerable AAA user authentication success logs will be printed, which may cause frequent screen refreshing or degrade the device performance. You can configure this command to disable the logging function.

Examples

The following example disables AAA user authentication success logging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no aaa log enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 aaa log rate-limit

Function

Run the **aaa log rate-limit** command to configure the rate of AAA user authentication success logging.

Run the **no** form of this command to restore the default configuration.

The default rate of AAA user authentication success logging is **5** logs/second.

Syntax

aaa log rate-limit *rate-limit*

no aaa log rate-limit

Parameter Description

rate-limit: Number of logs printed per second. The value range is from 0 to 65535 and the value **0** indicates that the logging rate is unlimited.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a large number of users go online, considerable AAA user authentication success logs will be printed, which may cause frequent screen refreshing or degrade the device performance. You can configure this command to adjust the rate of user authentication success logging.

Examples

The following example sets the rate of AAA user authentication success logging to **10** logs/second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa log rate-limit 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa log enable**

1.26 aaa new-model

Function

Run the **aaa new-model** command to enable AAA security services.

Run the **no** form of this command to disable this feature.

The AAA security services are disabled by default.

Syntax

aaa new-model

no aaa new-model

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable AAA security services. If AAA security services are disabled, AAA commands are unavailable.

Examples

The following example enables AAA security services.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa new-model
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 aaa user-role default

Function

Run the **aaa user-role default** command to configure the default role for AAA authorized users.

Run the **no** form of this command to restore the default configuration.

The default role of AAA authorized users is **network-operator**.

Syntax

aaa user-role default { *priv-level* | *role-name* | **network-admin** | **network-operator** }

no aaa user-role default

Parameter Description

priv-level: Privilege level of a user. The value is **priv-***n*, and *n* is a variable in the range of 0 to 15.

role-name: Custom user role.

network-admin: Uses the role **network-admin**, which has the administrator permissions.

network-operator: Uses the role **network-operator**, which has the operator permissions.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The RBAC function needs to be enabled first (run the **role enable** command in global configuration mode). For details about RBAC, see "Configuring RBAC" in the *Basic Configuration Command Reference*.

Examples

The following example sets the default role of AAA authorized users to **network-admin**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa user-role default network-admin
```

Notifications

N/A

Common Errors

N/A

Platform Description

Switching platform

Related Commands

- **role enable** (basic configuration/RBAC)

1.28 access-limit

Function

Run the **access-limit** command to configure a limit on the number of users supported in a domain.

Run the **no** form of this command to remove this configuration.

No limit on the number of users supported in a domain is configured by default.

Syntax

access-limit *access-limit-number*

no access-limit

Parameter Description

access-limit-number: Limit on the number of users supported in a domain. Only the number of IEEE 802.1X users is limited. The value range is from 1 to 1024.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the upper limit on the number of users supported in a domain named **domain.com** to **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
```

```
Hostname(config-aaa-domain)# access-limit 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**

1.29 accounting network

Function

Run the **accounting network** command to configure a network accounting method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default network accounting method list of an AAA domain is the default method list.

Syntax

accounting network { **default** | *list-name* }

no accounting network

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the network accounting method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# accounting network default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa accounting network**

1.30 accounting commands

Function

Run the **accounting commands** command to configure a command accounting method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default command accounting method list of an AAA domain is the default method list.

Syntax

accounting commands *level* { **default** | *list-name* }

no accounting commands *level*

Parameter Description

level: Level of commands that need authorization. The value range is from 0 to 15.

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the command accounting method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# accounting commands default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa accounting commands**

1.31 accounting exec

Function

Run the **accounting exec** command to configure an EXEC accounting method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default EXEC accounting method list of an AAA domain is the default method list.

Syntax

accounting exec { **default** | *list-name* }

no accounting exec

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the EXEC accounting method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# accounting exec default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa accounting exec**

1.32 authentication dot1x

Function

Run the **authentication dot1x** command to configure an IEEE 802.1X authentication method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default IEEE 802.1X authentication method list of an AAA domain is the default method list.

Syntax

authentication dot1x { **default** | *list-name* }

no authentication dot1x

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the IEEE 802.1X authentication method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authentication dot1x default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa authentication dot1x**

1.33 authentication login

Function

Run the **authentication login** command to configure a login authentication method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default login authentication method list of an AAA domain is the default method list.

Syntax

authentication login { **default** | *list-name* }

no authentication login

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the login authentication method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
```

```
Hostname(config-aaa-domain)# authentication login default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa authentication login**

1.34 authentication enable

Function

Run the **authentication enable** command to configure an Enable authentication method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default Enable authentication method list of an AAA domain is the default method list.

Syntax

authentication enable default

no authentication enable

Parameter Description

default: Uses the default method list. Only the default method list is supported currently.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the Enable authentication method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authentication enable default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa authentication enable default**

1.35 authorization network

Function

Run the **authorization network** command to configure a network authorization method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default network authorization method list of an AAA domain is the default method list.

Syntax

authorization network { **default** | *list-name* }

no authorization network

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

This command is used to specify a network authorization method list for an AAA domain. The domain-based AAA services need to be enabled for the execution of this command.

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the network authorization method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authorization network default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa authorization network**

1.36 authorization commands

Function

Run the **authorization commands** command to configure a command authorization method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default command authorization method list of an AAA domain is the default method list.

Syntax

authorization commands *level* { **default** | *list-name* }

no authorization commands *level*

Parameter Description

level: Level of commands that need authorization. Only authorized commands can be executed. The value range is from 0 to 15.

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the command authorization method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authorization commands default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**

1.37 authorization exec

Function

Run the **authorization exec** command to configure an EXEC authorization method list for an AAA domain.

Run the **no** form of this command to remove this configuration.

The default EXEC authorization method list of an AAA domain is the default method list.

Syntax

authorization exec { **default** | *list-name* }

no authorization exec

Parameter Description

default: Uses the default method list.

list-name: Name of a method list.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

If you configure this command repeatedly, the later configuration will overwrite earlier configuration.

Examples

The following example sets the EXEC authorization method list to the default method list for a domain named **domain.com**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authorization exec default
```

Notifications

If the name of a specified method list exceeds the length limit, the following notification will be displayed:

```
Method list name is too long
```

If the specified method list is not configured, the following notification will be displayed:

```
%WARNING: method list named XXX for this type is not existed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa domain enable**
- **aaa authorization exec**

1.38 clear aaa local user lockout

Function

Run the **clear aaa local user lockout** command to clear the list of locked users.

Syntax

clear aaa local user lockout { **all** | **user-name** *user-name-id* }

Parameter Description

all: Indicates all locked users.

user-name *user-name-id*: Specifies the ID of a locked user.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

You can clear a specified locked user or all locked users in the list.

Examples

The following example clears all locked users.

```
Hostname> enable
Hostname# clear aaa local user lockout all
```

Notifications

When you attempt to clear a specified user and the user exists, the following notification will be displayed:

```
User XXX unlocked
```

Platform Description

N/A

Related Commands

N/A

1.39 show aaa accounting update

Function

Run the **show aaa accounting update** command to display accounting update information.

Syntax

show aaa accounting update

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Accounting update information includes whether accounting update is enabled and the accounting update interval.

Examples

The following example displays accounting update information.

```
Hostname> enable
Hostname# show aaa accounting update
```

```
Accounting Update:         Disabled
Accounting Update Interval: 5 Minutes
```

Table 1-1 Output Fields of the show aaa accounting update Command

Field	Description
Accounting Update	Whether the accounting update function is enabled
Accounting Update Interval	Accounting update interval

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.40 show aaa domain

Function

Run the **show aaa domain** command to display information about a configured domain.

Syntax

show aaa domain [**default** | *domain-name*]

Parameter Description

default: Displays information about the default domain.

domain-name: Specified domain name. After this parameter is configured, information about the specified domain will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no domain name is specified, information about all domains will be displayed.

The parameter *domain-name* can be configured only after the domain-based AAA services are enabled. You can enable the domain-based AAA services by running the **aaa domain enable** command.

Examples

The following example displays information about the domain named **domain.com**.

```
Hostname> enable
Hostname# show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

Table 1-2 Output Fields of the show aaa domain Command

Field	Description
State	Status of the domain authentication function
Username format	Whether the username contains the domain name
Access limit	Whether the access is limited
802.1X Access statistic	Number of IEEE 802.1X-authenticated hosts that access the network
Selected method list	Domain authentication method list

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.41 show aaa lockout

Function

Run the **show aaa lockout** command to display lockout parameter configuration in the current login authentication.

Syntax

show aaa lockout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays lockout parameter configuration in the current login authentication.

```
Hostname> enable
Hostname# show aaa lockout
Lock tries:    3
Lock timeout:  15 minutes
```

Table 1-3 Output Fields of the show aaa lockout Command

Field	Description
Lock tries	Maximum number of login attempts
Lock timeout	Lockout duration after the number of consecutive failed login attempts of a user exceeds the configured value

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 show aaa group

Function

Run the **show aaa group** command to display all AAA server groups.

Syntax

show aaa group

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all AAA server groups.

```
Hostname> enable
Hostname# show aaa group
Type      Reference  Name
```

```
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          dot1x_group
radius     1          login_group
radius     1          enable_group
```

Table 1-4 Output Fields of the show aaa group Command

Field	Description
Type	Type of a server group
Reference	Number of times that the server group is referenced
Name	Name of the server group

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 show aaa method-list

Function

Run the **show aaa method-list** command to display all AAA method lists.

Syntax

show aaa method-list

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all AAA method lists.

```
Hostname> enable
Hostname# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorizating network default group radius
```

Table 1-5 Output Fields of the show aaa method-list Command

Field	Description
Authentication method-list	Authentication method list
Accounting method-list	Accounting method list
Authorization method-list	Authorization method list

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show aaa user

Function

Run the **show aaa user** command to display information about an AAA user.

Syntax

show aaa user { **all** | **by-id** *session-id* | **by-name** *user-name* | **lockout** }

Parameter Description

all: Displays information about all AAA users.

by-id *session-id*: Displays information about an AAA user with a specified session ID. The value range is from 1 to 2147483647.

by-name *user-name*: Displays information about an AAA user with a specified username.

lockout: Displays the list of locked AAA users.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about all AAA users.

```
Hostname> enable
Hostname# show aaa user all
-----------------------------
       Id ----- Name
 2345687901     wwxy
```

Table 1-6 Output Fields of the show aaa user all Command

Field	Description
Id	Unique session ID of a user
Name	Name of an authenticated user

The following example displays the list of locked AAA users.

```
Hostname> enable
Hostname# show aaa user lockout

Name                          Tries     Lock      Timeout(min)
```

```
------------------------------ ---------- ---------- ------------
```

Table 1-7 Output Fields of the show aaa user lockout Command

Field	Description
Name	Name of a locked user
Tries	Number of authentication attempts
Lock	Lockout status
Timeout(min)	Remaining time before unlocking

The following example displays information about an AAA user with the session ID 2345687901.

```
Hostname> enable
Hostname# show aaa user by-id 2345687901
----------------------------
       Id ----- Name
 2345687901     wwxy
```

Table 1-8 Output Fields of the show aaa user by-id Command

Field	Description
Id	Unique session ID of a user
Name	Name of the authenticated user searched out by session ID

The following example displays information about an AAA user with the username **wwxy**.

```
Hostname> enable
Hostname# show aaa user by-name wwxy
----------------------------
```

```
      Id ----- Name
2345687901     wwxy
```

Table 1-9 Output Fields of the show aaa user by-name Command

Field	Description
Id	Session ID searched out by username
Name	Name of an authenticated user

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 state

Function

Run the **state** command to configure the status of a domain.

Run the **no** form of this command to restore the default configuration.

A configured domain is active by default.

Syntax

state { **active** | **block** }

no state

Parameter Description

active: Sets a domain to be active.

block: Sets a domain to be inactive.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets a domain named **domain.com** to be inactive.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# state block
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 username-format

Function

Run the **username-format** command to configure whether usernames carry domain name information during interaction between the device and the server.

Run the **no** form of this command to restore the default configuration.

Usernames carry domain name information during interaction between the NAS and the server by default.

Syntax

username-format { **with-domain** | **without-domain** }

no username-format

Parameter Description

with-domain: Indicates that usernames carry domain name information.

without-domain: Indicates that usernames do not carry domain name information.

Command Modes

Domain configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures usernames not to carry domain name information during interaction between a domain named **domain.com** and the server.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# username-domain without-domain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 RADIUS Commands

Command	Function
aaa group server radius	Configure a Remote Authentication Dial-In User Service (RADIUS) server group.
ip radius source-interface	Configure the source IP address for RADIUS packets.
ip oob	Configure an MGMT port to be used by a RADIUS server group.
ip vrf forwarding	Specify a virtual routing and forwarding (VRF) instance for a RADIUS server group.
radius data-flow-format	Configure the units of data flows and data packets to be sent to a RADIUS server.
radius dscp	Configure the differentiated services code point (DSCP) value for RADIUS packets.
radius vendor-specific extend	Enable the function of not differentiating private vendor IDs during RADIUS packet parsing.
radius vendor-specific attribute support	Enable the function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets.
radius-server accounting-on enable	Enable the function of sending accounting-on packets upon device restart.
radius-server account update retransmit	Enable the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.
radius-server attribute 31	Configure the MAC address format for the Calling-Station-ID attribute of RADIUS.
radius-server attribute nas-port-id format	Configure the encapsulation format for the NAS-Port-ID attribute of RADIUS.
radius-server attribute class	Enable the function of parsing the rate limit configuration from the class attribute of RADIUS.
radius-server dead-criteria	Configure the criteria for the device to judge that a RADIUS server is unreachable.

radius-server deadtime	Configure the duration for the device to stop sending request packets to a RADIUS server when the server is unreachable.
radius-server host	Configure a RADIUS server.
radius-server key	Configure a shared key for the communication between the device and a RADIUS server.
radius-server retransmit	Configure the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable.
radius-server source-port	Configure the source port for the device to send RADIUS packets.
radius-server timeout	Configure the waiting time, after which the device retransmits a RADIUS request packet.
radius-server authentication attribute	Configure whether authentication request packets carry specified attributes.
radius-server account attribute	Configure whether RADIUS accounting request packets carry specified attributes.
radius-server authentication vendor	Configure authentication request packets to carry private attributes of other vendors.
radius-server accounting-copy	Enable the function of copying and sending RADIUS accounting packets to servers in a specified server group.
radius-server account vendor	Configure RADIUS accounting request packets to carry private attributes of other vendors.
radius set qos cos	Set the quality of service (QoS) value delivered by RADIUS to the class of service (CoS) value of an interface.
radius support cui	Enable RADIUS to support the CUI attribute.
server auth-port acct-port	Configure a server for a RADIUS server group.
show radius acct statistics	Display RADIUS accounting statistics.
show radius auth statistics	Display RADIUS authentication statistics.
show radius group	Display the configuration of a RADIUS server group.
show radius parameter	Display global parameters of a RADIUS server.
show radius server	Display the configuration of a RADIUS server.

show radius vendor-specific	Display the configurations of RADIUS private attribute types.
show radius attribute	Display RADIUS standard attributes.
show radius-server accounting-copy	Display the configuration of copying and sending accounting packets.

1.1 aaa group server radius

Function

Run the **aaa group server radius** command to configure a Remote Authentication Dial-In User Service (RADIUS) server group.

Run the **no** form of this command to remove this configuration.

No RADIUS server group is configured by default.

Syntax

aaa group server radius *group-name*

no aaa group server radius *group-name*

Parameter Description

group-name: Name of a server group.

Caution

The name of a server group cannot be the keyword **radius** or **tacacs+**. The two keywords are the default server group names of RADIUS and TACACS+ respectively.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an AAA server group of the RADIUS type, with the name **ss**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip radius source-interface

Function

Run the **ip radius source-interface** command to configure the source IP address for RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The source IP address of RADIUS packets is set by the network layer by default.

Syntax

ip radius source-interface *interface-type interface-number*

no ip radius source-interface

Parameter Description

interface-type interface-number: Interface type and interface number. The first IP address of the interface is used as the source IP address of RADIUS packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the device uses the first IP address of the interface specified in the command as the source address of RADIUS packets. Ensure that the communication between the configured IP address and a RADIUS server is normal. Specifying the source IP address for packets to be sent to a RADIUS server can reduce the NAS information maintenance workload on the RADIUS server.

Examples

The following example configures the first IP address of interface GigabitEthernet 0/1 as the source IP address of RADIUS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip radius source-interface gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip oob

Function

Run the **ip oob** command to configure an MGMT port to be used by a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No MGMT port to be used by a RADIUS server group is configured by default.

Syntax

ip oob [**via Mgmt** *Mgmt_number*]

no ip

Parameter Description

via Mgmt *Mgmt_number*: MGMT port to be used by a RADIUS server group. MGMT 0 is used by default.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates a server group named **ss** and sets the source interface to be used by the server group to send RADIUS packets to MGMT 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.14
Hostname(config-gs-radius)# server 192.168.4.15
Hostname(config-gs-radius)# ip oob via mgmt 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa group server radius**

1.4 ip vrf forwarding

Function

Run the **ip vrf forwarding** command to specify a virtual routing and forwarding (VRF) instance for a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No VRF instance is specified for a RADIUS server group by default.

Syntax

ip vrf forwarding *vrf-name*

no ip

Parameter Description

vrf-name: VRF instance used by a RADIUS server group.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

The VRF instance specified for a RADIUS server group must use a valid name configured using the **vrf definition** command in global configuration mode.

Examples

The following example sets the VRF instance used by a RADIUS server group named **ss** to **vrf-name**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12
Hostname(config-gs-radius)# server 192.168.4.13
Hostname(config-gs-radius)# ip vrf forwarding vrf-name
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa group server radius**

1.5 radius data-flow-format

Function

Run the **radius data-flow-format** command to configure the units of data flows and data packets to be sent to a RADIUS server.

Run the **no** form of this command to restore the default configuration.

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively.

Syntax

radius data-flow-format { { **data byte** | **data giga-byte** | **data kilo-byte** | **data mega-byte** } | { **packet giga-packet** | **packet kilo-packet** | **packet mega-packet** | **packet one-packet** } } *

no radius data-flow-format

Parameter Description

data byte: Sets the unit of data flows to bytes.

data giga-byte: Sets the unit of data flows to gigabytes.

data kilo-byte: Sets the unit of data flows to kilobytes.

data mega-byte: Sets the unit of data flows to megabytes.

packet giga-packet: Sets the unit of data packets to giga-packets.

packet kilo-packet: Sets the unit of data packets to kilo-packets.

packet mega-packet: Sets the unit of data packets to mega-packets.

packet one-packet: Sets the unit of data packets to packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the unit of data flows to be sent to a RADIUS server to kilobytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius data-flow-format data kilo-byte
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 radius dscp

Function

Run the **radius dscp** command to configure the differentiated services code point (DSCP) value for RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The default DSCP value of RADIUS packets is **0**.

Syntax

radius dscp *dscp-value*

no radius dscp

Parameter Description

dscp-value: DSCP value of RADIUS packets. The value range is from 0 to 63.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

DSCP is in the type of service (ToS) field of the IP header and is used to identify the packet transmission priority. A larger DSCP value indicates a higher packet priority. The default DSCP value of RADIUS packets is **0**. You can configure the DSCP value for RADIUS packets to change the transmission priority of RADIUS packets.

Examples

The following example sets the DSCP value of RADIUS packets to **2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius dscp 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 radius vendor-specific extend

Function

Run the **radius vendor-specific extend** command to enable the function of not differentiating private vendor IDs during RADIUS packet parsing.

Run the **no** form of this command to disable this feature.

The function of not differentiating private vendor IDs during RADIUS packet parsing is disabled and only Ruijie private vendor ID is identified by default.

Syntax

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of not differentiating private vendor IDs during RADIUS packet parsing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius vendor-specific extend
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 radius vendor-specific attribute support

Function

Run the **radius vendor-specific attribute support** command to enable the function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets.

Run the **no** form of this command to disable this feature.

The function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets is enabled by default.

Syntax

radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

no radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

Parameter Description

cisco: Supports the parsing of Cisco private attributes.

huawei: Supports the parsing of Huawei private attributes.

ms: Supports the parsing of Microsoft private attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the function of parsing Huawei private attributes carried in RADIUS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no radius vendor-specific attribute support huawei
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 radius-server accounting-on enable

Function

Run the **radius-server accounting-on enable** command to enable the function of sending accounting-on packets upon device restart.

Run the **no** form of this command to disable this feature.

The function of sending accounting-on packets upon device restart is enabled by default.

Syntax

radius-server accounting-on enable

no radius-server accounting-on enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The accounting-on function is used to notify a RADIUS server of the device restart. After the device is restarted, online users are forced offline. However, the RADIUS server does not perceive the device restart and does not log off the users. As a result, the users encounter an exception when initiating re-authentication. Therefore, it is necessary to enable the accounting-on function.

Examples

The following example enables the function of sending accounting-on packets upon device restart.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no radius-server accounting-on enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 radius-server account update retransmit

Function

Run the **radius-server account update retransmit** command to enable the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.

Run the **no** form of this command to disable this feature.

The function of retransmitting accounting update packets of 2nd-generation Web-authenticated users is enabled by default.

Syntax

radius-server account update retransmit

no radius-server account update retransmit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configuration does not affect users of other authentication types.

Examples

The following example enables the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account update retransmit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 radius-server attribute 31

Function

Run the **radius-server attribute 31** command to configure the MAC address format for the **Calling-Station-ID** attribute of RADIUS.

Run the **no** form of this command to restore the default configuration.

The MAC address format of the **Calling-Station-ID** attribute uses the unformatted pattern by default.

Syntax

radius-server attribute 31 mac format { **3hyphen** | **ietf** | **normal** | **unformatted** | { { **colon-split** | **dot-split** | **hyphen-split** } { **mode1** | **mode2** } [**lowercase** | **uppercase**] } }

no radius-server attribute 31 mac format

Parameter Description

3hyphen: Sets the MAC address format to 00d0-4096-3e4a.

ietf: Sets the MAC address format to the standard format specified in the Internet Engineering Task Force (IETF) standard (RFC3580). It uses hyphens (-) as the separator, for example, 00-D0-F8-33-22-AC.

normal: Sets the MAC address format to normal format, that is, dotted hexadecimal format using dots (.) as the separator, for example, 00d0.f833.22ac.

unformatted: Sets the MAC format type to unformatted pattern without separators, for example, 00d0f83322ac.

colon-split: Sets the MAC address format to a pattern using colons (:) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

dot-split: Sets the MAC address format to a pattern using dots (.) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

hyphen-split: Sets the MAC address format to a pattern using hyphens (-) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

mode1: Sets the MAC address format to a pattern using three groups with four characters in each group. It needs to be used together with **dot-split**, **colon-split**, and **hyphen-split**, for example, 00D0.F833.22AC, 00D0:F833:22AC, and 00D0-F833-22AC.

mode2: Sets the MAC address format to a pattern using six groups with two characters in each group. It needs to be used together with **dot-split**, **colon-split**, and **hyphen-split**, for example, 00.D0.F8.33.22.AC, 00:D0:F8:33:22:AC, and 00-D0-F8-33-22-AC.

lowercase: Sets the MAC address format to use lowercase letters.

uppercase: Sets the MAC address format to use uppercase letters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the uppercase/lowercase form is not specified for the MAC address format, the lowercase form is used by default.

Some RADIUS servers (mainly used for IEEE 802.1X authentication) can identify MAC addresses only in the IETF format. In this case, set the MAC address format of **Calling-Station-ID** to IETF.

Examples

The following example sets the MAC address format of the **Calling-Station-ID** attribute to IETF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute 31 mac format ietf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 radius-server attribute nas-port-id format

Function

Run the **radius-server attribute nas-port-id format** command to configure the encapsulation format for the **NAS-Port-ID** attribute of RADIUS.

Run the **no** form of this command to restore the default configuration.

The **NAS-Port-ID** attribute of RADIUS uses the normal encapsulation format by default.

Syntax

radius-server attribute nas-port-id format { **mode1** | **normal** | **port-vid** | **qinq** }

no radius-server attribute nas-port-id format

Parameter Description

mode1: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS. The format is slot = XX; subslot = XX; port = XXX; VLAN ID = XXXX. If the range of a user interface is beyond 255, this format cannot be used. Parameters in this format are described as follows:

- **slot**: Indicates the device ID. The value range is from 0 to 15.
- **subslot**: Indicates the slot ID. The value range is from 0 to 15.
- **port**: Indicates the port ID. The value range is from 0 to 255.
- **VLAN ID**: Indicates the VLAN ID. The value range is from 1 to 4094.

normal: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS. The format is %Interface_name%. **Interface_name** refers to the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.

port-vid: Sets the encapsulation format to port-vid. The format is %Interface%:%vid%. Parameters in the format are described as follows:

- **Interface**: Indicates the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.
- **vid**: Indicates the ID of a user VLAN.

qinq: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS.

Format without an inner VID: %Interface_name%.%outer_vid4%%tag%:%outer_vid%.

Format with an inner VID: %Interface_name%.%outer_vid4%%inner_vid4%:%outer_vid%-%inner_vid%.

Parameters in the format are described as follows:

- **Interface_name**: Indicates the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.
- **outer_vid4**: Indicates the outer VLAN ID (it occupies four digits and spaces are filled in when there are less than four digits).
- **inner_vid4**: Indicates the inner VLAN ID (it occupies four digits and spaces are filled in when there are less than four digits).
- **tag**: Indicates a tag and the value is **0** (it occupies four digits and spaces are filled in when there are less than four digits).
- **outer_vid**: Indicates the outer VLAN ID (the number of digits is not limited, and the actual number is printed. For example, 10 is printed for VLAN 10).
- **inner_vid**: Indicates the inner VLAN ID (the number of digits is not limited, and the actual number is printed. For example, 10 is printed for VLAN 10).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the encapsulation format of the **NAS-Port-ID** attribute of RADIUS to QinQ format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute nas-port-id format qinq
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 radius-server attribute class

Function

Run the **radius-server attribute class** command to enable the function of parsing the rate limit configuration from the **class** attribute of RADIUS.

Run the **no** form of this command to disable this feature.

The function of parsing the rate limit configuration from the **class** attribute of RADIUS is disabled by default.

Syntax

radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** | **unit bit/s** | **unit byte/s** }}

no radius-server attribute class user-flow-control

Parameter Description

format-16bytes: Sets the format of the rate limit value parsed from the **class** attribute to 16 bytes.

format-32bytes: Sets the format of the rate limit value parsed from the **class** attribute to 32 bytes.

unit bit/s: Sets the format of the rate limit value parsed from the **class** attribute to bps.

unit byte/s: Sets the format of the rate limit value parsed from the **class** attribute to bytes/s.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of parsing the rate limit configuration from the **class** attribute of RADIUS and sets the format of the parsed rate limit value to 32 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute class user-flow-control format-32bytes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 radius-server dead-criteria

Function

Run the **radius-server dead-criteria** command to configure the criteria for the device to judge that a RADIUS server is unreachable.

Run the **no** form of this command to restore the default configuration.

The criteria for judging that a RADIUS server is unreachable are that the timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

Syntax

radius-server dead-criteria { **time** *timeout* | **tries** *tries-number* | **time** *timeout* **tries** *tries-number* }

no radius-**server dead**-**criteria** { **time** | **tries** | **time tries** }

Parameter Description

time *timeout*: Configures the timeout duration, in seconds. The value range is from 1 to 120. If the device fails to receive a correct response packet from a RADIUS server within the specified time, it is deemed that the RADIUS server meets the unreachability duration condition.

tries *tries-number*: Configures the consecutive timeout count. The value range is from 1 to 100. When the consecutive timeout count of request packets sent by the device to the same RADIUS server reaches the configured count, it is deemed that the RADIUS server meets the consecutive timeout count condition of unreachability.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If a RADIUS server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS server is unreachable. You can use this command to adjust the timeout duration and consecutive request timeout count.

Examples

The following example configures the criteria for judging that a RADIUS server is unreachable as follows: The timeout duration is **120** seconds and the consecutive timeout count to **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server dead-criteria time 120 tries 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 radius-server deadtime

Function

Run the **radius-server deadtime** command to configure the duration for the device to stop sending request packets to a RADIUS server when the server is unreachable.

Run the **no** form of this command to restore the default configuration.

Even if a RADIUS server is unreachable, the device still sends requests to the RADIUS server by default.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameter Description

deadtime: Duration for the device to stop sending requests to an unreachable RADIUS server, in minutes. The value range is from 1 to 1440.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If active detection is enabled for a RADIUS server on the device, the time parameter configured by the **radius-server deadtime** command does not take effect on the RADIUS server. Otherwise, if the duration in which the RADIUS server is unreachable exceeds the time specified by the **radius-server deadtime** command, the device automatically restores the RADIUS server to the reachable state.

Examples

The following example sets the duration for the device to stop sending request packets to an unreachable RADIUS server to **1** minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server deadtime 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 radius-server host

Function

Run the **radius-server host** command to configure a RADIUS server.

Run the **no** form of this command to remove this configuration.

No RADIUS server is configured by default.

Syntax

radius-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

no radius-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

Parameter Description

oob: Configures the device to use an MGMT port to send RADIUS packets. MGMT 0 is used for sending RADIUS packets by default.

via Mgmt *mgmt-numb*: Configures an MGMT port as the source interface for sending packets to a RADIUS server.

ipv4-address: Configures an IPv4 address for the RADIUS server.

ipv6-address: Configures an IPv6 address for the RADIUS server.

auth-port *auth-port-number*: Configures the UDP port for RADIUS authentication. The value range is from 0 to 65535 and the value **0** indicates that the server does not perform authentication.

acct-port *acct-port-number*: Configures the UDP port for RADIUS accounting. The value range is from 0 to 65535 and the value **0** indicates that the server does not perform accounting.

test username *username*: Enables the active detection function for the RADIUS server and specifies the username used in active detection.

ignore-auth-port: Disables the function of detecting the authentication port of the RADIUS server. Authentication port detection is enabled by default.

ignore-acct-port: Disables the function of detecting the accounting port of the RADIUS server. Accounting port detection is enabled by default.

idle-time *idle-minutes*: Configures the interval for the device to send test packets to a reachable RADIUS server, in minutes. The value range is from 1 to 1440 and the default value is **60**.

key [**0** | **7**] *text-string*: Configures a shared key for the server. The global shared key is used by default. You can specify the encryption type for the configured key. The value **0** indicates no encryption, **7** indicates simple encryption, and **0** is used by default.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the Advanced Encryption Standard (AES)-128/Secure Hash Algorithm (SHA)-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

A RADIUS server must be defined to implement the AAA security service by using RADIUS. You can use this command to define one or more RADIUS servers.

If a RADIUS server is not added to a RADIUS server group, the device uses the global routing table when sending RADIUS packets to the RADIUS server. Otherwise, the device uses the VRF routing table of the RADIUS server group.

Examples

The following example configures a RADIUS server in an IPv4 environment.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 192.168.12.1
```

The following example configures a RADIUS server in an IPv4 environment, enables active detection, sets the detection interval to **60** minutes, and disables accounting UDP port detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 192.168.100.1 test username test idle-time 60
ignore-acct-port
```

The following example configures a RADIUS server in an IPv6 environment.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 3000::100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 radius-server key

Function

Run the **radius-server key** command to configure a shared key for the communication between the device and a RADIUS server.

Run the **no** form of this command to remove this configuration.

No shared key for the communication between the device and a RADIUS server is configured by default.

Syntax

radius-server key [**0** | **7**] *key*

no radius-server key

Parameter Description

0 | **7**: Configures the encryption type of a key. The value **0** indicates no encryption and **7** indicates simple encryption.

key: Text of a shared key.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the Advanced Encryption Standard (AES)-128/Secure Hash Algorithm (SHA)-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

A shared key is the basis for correct communication between the device and a RADIUS server. The same shared key must be configured on the device and a RADIUS server so that they can communicate with each other successfully.

Examples

The following example sets the shared key for the communication between the NAS and a RADIUS server to **aaa**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server key aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 radius-server retransmit

Function

Run the **radius-server retransmit** command to configure the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable.

Run the **no** form of this command to restore the default configuration.

The device retransmits packets to a RADIUS server three times before confirming that the RADIUS server is unreachable by default.

Syntax

radius-server retransmit *retransmit-times*

no radius-server retransmit

Parameter Description

retransmit-times: Packet retransmission count before the device confirms that a RADIUS server is unreachable. The value range is from 0 to 100 and the value **0** indicates no retransmission.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the duration, in which the device retransmits RADIUS packets for a specified number of times. There is a timeout interval between two consecutive retransmissions.

Examples

The following example sets the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server retransmit 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 radius-server source-port

Function

Run the **radius-server source-port** command to configure the source port for the device to send RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The source port used by the device to send RADIUS packets is a random port by default.

Syntax

radius-server source-port *source-port*

no radius-server source-port

Parameter Description

source-port: Source port used by the device to send RADIUS packets. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source port used by the device to send RADIUS packets is a random port by default. You can run this command to specify the source port.

Examples

The following example sets the source port for the device to send RADIUS packets to **10000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server source-port 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 radius-server timeout

Function

Run the **radius-server timeout** command to configure the waiting time, after which the device retransmits a RADIUS request packet.

Run the **no** form of this command to restore the default configuration.

The default waiting time before the retransmission of a RADIUS packet is **5** seconds.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameter Description

timeout: Response timeout duration of a security server, in seconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the waiting time, after which the device retransmits a RADIUS request packet, to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server timeout 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 radius-server authentication attribute

Function

Run the **radius-server authentication attribute** command to configure whether authentication request packets carry specified attributes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Whether RADIUS authentication request packets carry specified attributes is consistent with the stipulation in the RFC standard by default.

Syntax

radius-server authentication attribute *type* { **package** | **unpackage** }

no radius-server authentication attribute *type* { **package** | **unpackage** }

default radius-server authentication attribute *type* { **package** | **unpackage** }

Parameter Description

type: Type of a RADIUS attribute. The value range is from 1 to 255.

package: Indicates that RADIUS authentication request packets carry specified attributes.

unpackage: Indicates that RADIUS authentication request packets do not carry specified attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS authentication request packets not to carry attribute 87.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server authentication attribute 87 unpackage
```

Related Commands

N/A

1.22 radius-server account attribute

Function

Run the **radius-server account attribute** command to configure whether RADIUS accounting request packets carry specified attributes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Whether RADIUS accounting request packets carry specified attributes is consistent with the stipulation in the RFC standard by default.

Syntax

radius-server account attribute *type* { **package | unpackage** }

no radius-server account attribute *type* { **package | unpackage** }

default radius-server account attribute *type* { **package | unpackage** }

Parameter Description

type: Type of a RADIUS attribute. The value range is from 1 to 255.

package: Indicates that RADIUS accounting request packets carry specified attributes.

unpackage: Indicates that RADIUS accounting request packets do not carry specified attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS accounting request packets not to carry attribute 87.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account attribute 87 unpackage
```

Related Commands

N/A

1.23 radius-server authentication vendor

Function

Run the **radius-server authentication vendor** command to configure authentication request packets to carry private attributes of other vendors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Authentication request packets do not carry private attributes of other vendors by default.

Syntax

radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

no radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

default radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

Parameter Description

cisco: Indicates that Cisco private attributes are carried.

cmcc: Indicates that CMCC private attributes are carried.

microsoft: Indicates that Microsoft private attributes are carried.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures authentication request packets to carry CMCC private attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server authentication vendor cmcc package
```

Related Commands

N/A

1.24 radius-server accounting-copy

Function

Run the **radius-server accounting-copy** command to enable the function of copying and sending RADIUS accounting packets to servers in a specified server group.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The function of copying and sending RADIUS accounting packets is disabled by default.

Syntax

radius-server accounting-copy *group*

no radius-server accounting-copy *group*

Parameter Description

group: Server group, to which accounting packets are to be sent.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of copying and sending RADIUS accounting packets to servers in a server group named **cpy-grp**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# radius-server accounting-copy cpy-grp
```

Related Commands

N/A

1.25 radius-server account vendor

Function

Run the **radius-server account vendor** command to configure RADIUS accounting request packets to carry private attributes of other vendors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Accounting request packets do not carry private attributes of other vendors by default.

Syntax

radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

no radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

default radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

Parameter Description

cisco: Sets the vendor type to Cisco.

cmcc: Sets the vendor type to CMCC.

microsoft: Sets the vendor type to Microsoft.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS accounting request packets to carry CMCC private attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account vendor cmcc package
```

Related Commands

N/A

1.26 radius set qos cos

Function

Run the **radius set qos cos** command to set the quality of service (QoS) value delivered by RADIUS to the class of service (CoS) value of an interface.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The QoS value delivered by RADIUS is the DSCP value by default.

Syntax

radius set qos cos

no radius set qos cos

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the QoS value delivered by RADIUS to the CoS value of an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius set qos cos
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 radius support cui

Function

Run the **radius support cui** command to enable RADIUS to support the CUI attribute.

Run the **no** form of this command to disable this feature.

The function of supporting the CUI attribute by RADIUS is disabled by default.

Syntax

radius support cui

no radius support cui

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables RADIUS to support the CUI attribute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius support cui
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 server auth-port acct-port

Function

Run the **server auth-port acct-port** command to configure a server for a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No server is configured for a RADIUS server group by default.

Syntax

server { *ipv4-address* | *ipv6-address* } [**acct-port** *acct-port* | **auth-port** *auth-port*] *

no server { *ipv4-address* | *ipv6-address* } [**acct-port** *acct-port* | **auth-port** *auth-port*] *

Parameter Description

Ipv4-address: IPv4 address of a server.

Ipv6-address: IPv6 address of a server.

acct-port *acct-port*: Configures the accounting port ID for the server. The value range is from 1 to 65535, and the default value is **1813**.

auth-port *auth-port*: Configures the authentication port ID for the server. The value range is from 1 to 65535, and the default value is **1812**.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example adds a server with the IP address 192.168.4.12 to a server group named **ss**, sets the authentication port ID of the server to 10000, and the accounting port ID to 10001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12 acct-port 10000 auth-port 10001
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **radius-server deadtime**

1.29 show radius acct statistics

Function

Run the **show radius acct statistics** command to display RADIUS accounting statistics.

Syntax

show radius acct statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS accounting statistics.

```
Hostname> enable
Hostname# show radius acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 1
```

Table 1-1 Output Fields of the show radius radius acct statistics Command

Field	Description
Accounting Servers	Accounting server
Server Index	Server index
Server Address	IP address of the server
Server Port	Server port

Field	Description
Msg Round Trip Time	Duration from the time that an access request is sent to the server to the time an access response is received from the server
First Requests	Number of times that the first request is sent to the server
Retry Requests	Packet transmission count
Accounting Responses	Number of times that accounting response packets are received
Malformed Msgs	Number of RADIUS Access-Response error packets received from the server
Bad Authenticator Msgs	Number of packets with verification errors
Pending Requests	Number of RADIUS access request packets sent to the server, for which no timeout occurs and no response is received ● The value of this variable increases when an access request is sent. ● The value of this variable decreases when an access acceptance, access denial, access challenge, timeout, or retransmission message is received.

Notifications

N/A

Platform Description

N/A

1.30 show radius auth statistics

Function

Run the **show radius auth statistics** command to display RADIUS authentication statistics.

Syntax

show radius auth statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS authentication statistics.

```
Hostname> enable
Hostname# show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1812
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Table 1-2 Output Fields of the show radius radius auth statistics Command

Field	Description
Authentication Servers	Authentication server
Server Index	Server index
Server Address	Server address
Server Port	Server port ID
Msg Round Trip Time	Duration from the time that an access request is sent to the server to the time an access response is received from the server
First Requests	Number of times that the first request is sent
Retry Requests	Retransmission count
Accept Responses	Number of times that the Access-accept message is received
Reject Responses	Number of times that the Reject message is received
Challenge Responses	Number of times that the Challenge response message is received
Malformed Msgs	Number of RADIUS Access-Response error packets received from the server
Bad Authenticator Msgs	Number of packets with verification errors
Pending Requests	Number of RADIUS access request packets sent to the server, for which no

Field	Description
	timeout occurs and no response is received ● The value of this variable increases when an access request is sent. ● The value of this variable decreases when an access acceptance, access denial, access challenge, timeout, or retransmission message is received.
Timeout Requests	Number of timeout request times
Unknowntype Msgs	Number of packets of the unknown type
Other Drops	Number of other discarded packets

Notifications

N/A

Platform Description

N/A

1.31 show radius group

Function

Run the **show radius group** command to display the configuration of a RADIUS server group.

Syntax

show radius group

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of a RADIUS server group.

```
Hostname> enable
Hostname# show radius group
==========Radius group radius==========
Vrf:not-set
```

```
Server:192.168.1.1
  Server key:aaaa
  Authentication port:1812
  Accounting port:1813
  State:Active
```

Table 1-3 Output Fields of the show radius group Command

Field	Description
Vrf	VRF instance
Server	Server address
Server key	Server key
Authentication port	Authentication port
Accounting port	Accounting port
State	Server status

Notifications

N/A

Platform Description

N/A

1.32 show radius parameter

Function

Run the **show radius parameter** command to display global parameters of a RADIUS server.

Syntax

show radius parameter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays global parameters of a RADIUS server.

```
Hostname> enable
Hostname# show radius parameter
Server Timout:   5 Seconds
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:       10 Seconds
Tries:      10
```

Table 1-4 Output Fields of the show radius parameter Command

Field	Description
Server Timout	Waiting time prior to request retransmission
Server Deadtime	Duration for the device to stop sending request packets to an unreachable RADIUS server
Server Retries	Number of times that the device sends requests consecutively before confirming that a RADIUS server is unreachable
Server Dead Criteria	Criteria for judging that a RADIUS server is unreachable
Time	If the device fails to receive a correct response packet from a RADIUS server within the time, it is judged that the RADIUS server meets the unreachability duration condition.
Tries	When the number of times that the device sends a request packet to the RADIUS server consecutively reaches the configured value, it is judged that the RADIUS server meets the consecutive timeout count condition of unreachability.

Notifications

N/A

Platform Description

N/A

1.33 show radius server

Function

Run the **show radius server** command to display the configuration of a RADIUS server.

Syntax

show radius server

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of a RADIUS server.

```
Hostname> enable
Hostname# show radius server
Server IP:   192.168.4.12
Accounting  Port:  23
Authen  Port:    77
Test Username:   test
Test Idle Time:   10 Minutes
Test Ports:       Authen
Server State:    Active
   Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0
Server IP:   192.168.4.13
Accounting Port:  45
Authen  Port:    74
Test Username:   <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:       Authen and Accounting
Server State:    Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Table 1-5 Output Fields of the show radius server Command

Field	Description

Field	Description
Server IP	Server IP address
Accounting Port	Accounting port
Authen Port	Authentication port
Test Username	Username used for active detection
Test Idle Time	Interval for sending test packets to a reachable RADIUS server
Test Ports	Port for sending test packets
Server State	Server status
Dead	Total duration in which the server is unreachable and number of times that the server is unreachable
Statistics	Statistical data
Authen	Number of authentication requests
Author	Number of authorization requests
Account	Number of accounting requests
Server IP	Server IP address
Accounting Port	Accounting port
Authen Port	Authentication port
Test Username	Username used for active detection
Test Idle Time	Interval for sending test packets to a reachable RADIUS server
Test Ports	Port for sending test packets
Server State	Server status

Notifications

N/A

Platform Description

N/A

1.34 show radius vendor-specific

Function

Run the **show radius vendor-specific** command to display the configurations of RADIUS private attribute types.

Syntax

show radius vendor-specific

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays configurations of RADIUS private attribute types.

```
Hostname> enable
Hostname# show radius vendor-specific
id    vendor-specific     type-value
-------------
1     max-down-rate       1
2     port-priority       2
3     user-ip             3
4     VLAN-id             4
5     last-supplicant-vers 5
      ion
6     net-ip              6
7     user-name           7
8     password            8
9     file-directory      9
10    file-count          10
11    file-name-0         11
12    file-name-1         12
13    file-name-2         13
14    file-name-3         14
15    file-name-4         15
16    max-up-rate         16
17    current-supplicant-v 17
      ersion
18    flux-max-high32     18
19    flux-max-low32      19
20    proxy-avoid         20
21    dialup-avoid        21
22    ip-privilege        22
23    login-privilege     42
```

```
26   ipv6-multicast-addre 79
     ss
27   ipv4-multicast-addre 87
     ss
```

Table 1-6 Output Fields of the show radius vendor-specific Command

Field	Description
id	Serial number
vendor-specific	Private attribute meaning
type-value	ID of a private attribute

Notifications

N/A

Platform Description

N/A

1.35 show radius attribute

Function

Run the **show radius attribute** command to display RADIUS standard attributes.

Syntax

show radius attribute

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS standard attributes.

```
Hostname> enable
Hostname# show radius attribute
type        implicate
----        ---------
```

```
 1.........User-Name
 2.........User-Password
 3.........Chap-Password
 4.........NAS-Ip-Addr
 5.........Nas-Ip-Port
 6.........Service-Type
 7.........Framed-Protocol
 8.........Frame-Ip-Address
 9.........Framed-Ip-Mask
10.........Framed-Routing
11.........Filter-Id
12.........Framed-Mtu
13.........Framed-Compress
14.........Login-Ip-Host
15.........Login-Service
16.........Login-Tcp-Port
18.........Reply-Message
19.........Callback-Num
20.........Callback-Id
22.........Framed-Route
23.........Framed-IPX-Network
24.........State
25.........Class
26.........Vendor-Specific
27.........Session-Timeout
28.........Idle-Timeout
29.........Termination-Action
30.........Called-Station-Id
31.........Calling-Station-Id
32.........Nas-Id
33.........Proxy-State
34.........Login-LAT-Service
35.........Login-LAT-Node
36.........Login-LAT-Group
37.........Framed-AppleTalk-Link
38.........Framed-AppleTalk-Net
39.........Framed-AppleTalk-Zone
40.........Acct-Status-Type
41.........Acct-Delay-Time
42.........Acct-Input-Octets
43.........Acct-Output-Octets
44.........Acct-Session-Id
45.........Acct-Authentic
46.........Acct-Session-Time
47.........Acct-Input-Packet
48.........Acct-Output-Packet
```

```
 49..........Acct-Terminate-Cause
 50..........Acct-Multi-Session-ID
 51..........Acct-Link-Count
 52..........Acct-Input-Gigawords
 53..........Acct-Output-Gigawords
 60..........Chap-Challenge
 61..........Nas-Port-Type
 62..........Port-Limit
 63..........Login-Lat-Port
 64..........Tunnel-Type
 65..........Tunnel-Medium-Type
 66..........Tunnel-Client-EndPoint
 67..........Tunnel-Service-EndPoint
 79..........eap msg
 80..........Message-Authenticator
 81..........group id
 85..........Acct-Interim-Interval
 87..........Nas-Port-Id
 89..........cui
 95..........Nas-Ipv6-Addr
 96..........Framed-Interface-Id
 97..........Framed-Ipv6-Prefix
 98..........Login-Ipv6-Host
 99..........Framed-Ipv6-Route
100..........Framed-Ipv6-Pool
168..........Framed-Ipv6-Addr
```

Table 1-7 Output Fields of the show radius attribute Command

Field	Description
type	Serial number
implicate	Meaning of a standard attribute

Notifications

N/A

Platform Description

N/A

1.36 show radius-server accounting-copy

Function

Run the **show radius-server accounting-copy** command to display the configuration of copying and sending accounting packets.

Syntax

show radius-server accounting-copy

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of copying and sending accounting packets.

```
Hostname> enable
Hostname# show radius-server group-attribute
```

Notifications

N/A

Platform Description

N/A

1 TACACS Commands

Command	Function
aaa group server tacacs+	Configure a Terminal Access Controller Access Control System Plus (TACACS+) server group.
ip tacacs source-interface	Configure the source address for TACACS+ packets.
ip oob	Configure an MGMT port to be used by a TACACS+ server group.
ip vrf forwarding	Specify a VRF instance for a TACACS+ server group.
server	Add a server to a TACACS+ server group.
nas-ip	Enable the function of carrying the nas-ip attribute in packets.
show tacacs	Display the interaction between the device and each TACACS+ server.
tacacs-server host	Configure a TACACS+ server.
tacacs-server key	Configure a shared key for the communication between a network access server (NAS) and a TACACS+ server.
tacacs-server timeout	Configure the global timeout duration for a TACACS+ server in the communication between the device and the TACACS+ server.
tacacs-server dead-criteria	Configure the criteria for the device to judge that a TACACS+ server is unreachable.
tacacs-server deadtime	Configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

1.1 aaa group server tacacs+

Function

Run the **aaa group server tacacs+** command to configure a Terminal Access Controller Access Control System Plus (TACACS+) server group.

Run the **no** form of this command to remove this configuration.

No TACACS+ server group is configured by default.

Syntax

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Parameter Description

group-name: Name of a TACACS+ server group. The value is a string of 1 to 63 characters. The name cannot be set to the default name **radius** or **tacacs+**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can group TACACS+ servers so that authentication, authorization, and accounting can be completed by different server groups.

Examples

The following example configures a TACACS+ server group named **tac1**, and adds a TACACS+ server with the IP address 1.1.1.1 to the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs+)# server 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip tacacs source-interface

Function

Run the **ip tacacs source-interface** command to configure the source address for TACACS+ packets.

Run the **no** form of this command to remove this configuration.

No source address is configured for TACACS+ packets and the address is set by the network layer by default.

Syntax

ip tacacs source-interface *interface-type interface-number*

no ip tacacs source-interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to configure the source IP address for TACACS+ packets to be sent to a TACACS+ server, to reduce the network access server (NAS) information maintenance workload on the TACACS+ server. This command uses the first IP address of a specified interface as the source address of TACACS+ packets. If a specified interface belongs to a virtual routing and forwarding (VRF) instance, routes in the VRF instance are used to send packets.

Examples

The following example configures the IP address of interface GigabitEthernet 0/1 as the source address of TACACS+ packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tacacs source-interface gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip oob

Function

Run the **ip oob** command to configure an MGMT port to be used by a TACACS+ server group.

Run the **no** form of this command to remove this configuration.

No MGMT port to be used by a TACACS+ server group is configured by default.

Syntax

ip oob [**via Mgmt** *mgmt-number*]

no ip

Parameter Description

via Mgmt *mgmt-number*: Configures the number of an MGMT port to be used. MGMT 0 is used by default.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the MGMT port to be used by a TACACS+ server group named **ss** to MGMT 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ ss
Hostname(config-gs-tacacs+)# server 192.168.1.2
Hostname(config-gs-tacacs+)# ip oob via mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip vrf forwarding

Function

Run the **ip vrf forwarding** command to specify a VRF instance for a TACACS+ server group.

Run the **no** form of this command to remove this configuration.

No VRF instance is specified for a TACACS+ server group by default.

Syntax

ip vrf forwarding *vrf-name*

no ip

Parameter Description

vrf-name: VRF instance used by a server group.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

The VRF instance specified for a TACACS+ server group must use a valid name configured using the **vrf definition** command in global configuration mode.

Examples

The following example sets the VRF instance used by a TACACS+ server group to **vrf-name**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ ss
Hostname(config-gs-tacacs+)# server 192.168.1.2
Hostname(config-gs-tacacs+)# ip vrf forwarding vrf-name
```

Notifications

If the name of a specified VRF instance exceeds the length limit, the following notification will be displayed:

```
Name is too long
```

If a specified VRF instance is not configured, the following notification will be displayed:

```
Invalid vrf
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrf definition** (IP routing/VRF)

1.5 server

Function

Run the **server** command to add a server to a TACACS+ server group.

Run the **no** form of this command to remove this configuration.

No server is added to a TACACS+ server group by default.

Syntax

server { *ipv4-address* | *ipv6-address* }

no server { *ipv4-address* | *ipv6-address* }

Parameter Description

ipv4-address: IPv4 address of a server.

Ipv6-address: IPv6 address of a server.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to the next server in the server group.

Examples

The following example configures a TACACS+ server group named **tac1**, and adds a TACACS+ server with the IP address 192.168.1.2 to the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs+)# server 192.168.1.2
```

Notifications

When a server is added to a server group but the server is not configured, the following notification will be displayed:

```
Warning: Server 1.1.1.1 is not defined.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa group server tacacs+**

1.6 nas-ip

Function

Run the **nas-ip** command to enable the function of carrying the **nas-ip** attribute in packets.

Run the **no** form of this command to disable this feature.

Packets do not carry the **nas-ip** attribute by default.

Syntax

nas-ip { *ipv4-address* | *ipv6-address* }

no nas-ip { *ipv4-address* | *ipv6-address* }

Parameter Description

ipv4-address: **nas-ip** attribute value of an IPv4 address.

Ipv6-address: **nas-ip** attribute value of an IPv6 address.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a TACACS+ server group named **tac1** and enables the function of carrying the **nas-ip** attribute in packets for the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs+)# nas-ip 192.168.197.215
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa group server tacacs+**

1.7 show tacacs

Function

Run the **show tacacs** command to display the interaction between the device and each TACACS+ server.

Syntax

show tacacs

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the interaction between the device and each TACACS+ server.

```
Hostname> enable
Hostname# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Table 1-1 Output Fields of the show tacacs Command

Field	Description
Tacacs+ Server	Address of a TACACS+ server
Socket Opens	Number of established socket connections
Socket Closes	Number of released socket connections
Total Packets Sent	Number of sent packets

Field	Description
Total Packets Recv	Number of received packets
Reference Count	Server reference count

Notifications

N/A

Platform Description

N/A

1.8 tacacs-server host

Function

Run the **tacacs-server host** command to configure a TACACS+ server.

Run the **no** form of this command to remove this configuration.

No TACACS+ server is configured by default.

Syntax

tacacs-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**port** *port-number*] [**test username** *username*] [**idle-time** *idle-time*] [**timeout** *timeout*] [**key** [**0** | **7**] *key*]

no tacacs-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* }

Parameter Description

oob: Uses an MGMT port for communication. If this parameter is not specified, a non-MGMT port is used for communication.

via Mgmt *mgmt-number*: Specifies an MGMT port. If this parameter is not specified, MGMT 0 is used.

ipv4-address: IPv4 address of a TACACS+ server.

ipv6-address: IPv6 address of a TACACS+ server.

port *port-number*: Configures a TCP port for TACACS+ communication. The value range is from 1 to 65535, and the default value is **49**.

test username *username*: Configures a username used for detection. The value is a string of 1 to 63 characters.

idle-time *idle-time*: Configures the detection interval, in minutes. The value range is from 1 to 1440 and the default value is **60**.

timeout *timeout*: Configures the communication timeout duration of a TACACS+ server, in seconds. The value range is from 1 to 1000. If this parameter is not specified, the global timeout duration is used.

key [**0** | **7**] *key*: Configures a shared key for the server. You can specify the encryption type for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The value **0** is used by default. If this parameter is not specified, the global shared key is used.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the Advanced Encryption Standard (AES)-128/Secure Hash Algorithm (SHA)-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

Examples

The following example configures a TACACS+ server with the IPv4 address 192.168.12.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tacacs-server host 192.168.12.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 tacacs-server key

Function

Run the **tacacs-server key** command to configure a shared key for the communication between a network access server (NAS) and a TACACS+ server.

Run the **no** form of this command to remove this configuration.

No shared key for the communication between a NAS and a TACACS+ server is configured by default.

Syntax

tacacs-server key [**0** | **7**] *key*

no tacacs-server key

Parameter Description

0 | **7**: Configures the encryption type of a key. The value **0** indicates no encryption and **7** indicates simple encryption. If this parameter is not specified, no encryption is adopted.

key: Text of a shared key. The value is a string of 1 to 128 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the AES-128/SHA-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

This command is used to configure a global shared key. You can use the **key** field in the **tacacs-server host** command to specify different keys for servers.

Examples

The following example sets the shared key for the communication between the NAS and a TACACS+ server to **aaa**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tacacs-server key aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **tacacs-server host**

1.10 tacacs-server timeout

Function

Run the **tacacs-server timeout** command to configure the global timeout duration for a TACACS+ server in the communication between the device and the TACACS+ server.

Run the **no** form of this command to restore the default configuration.

The default timeout duration of a TACACS+ server is **5** seconds in the communication between the device and the TACACS+ server.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameter Description

timeout: Global timeout duration of a server, in seconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the global server response timeout duration. You can use the **timeout** field in the **tacacs-server host** command to specify different timeout duration values for servers.

Examples

The following example sets the global timeout duration to **10** seconds for a TACACS+ server in the communication between the device and the TACACS+ server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tacacs-server timeout 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **tacacs-server host**

1.11 tacacs-server dead-criteria

Function

Run the **tacacs-server dead-criteria** command to configure the criteria for the device to judge that a TACACS+ server is unreachable.

Run the **no** form of this command to restore the default configuration.

The criteria for the device to judge that a TACACS+ server is unreachable are that the server timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

Syntax

tacacs-server dead-criteria { **time** *timeout* **tries** *tries-number* | **time** *timeout* | **tries** *tries-number* }

no tacacs-server dead-criteria { **time tries** | **time** | **tries** }

Parameter Description

time *timeout*: Configures the timeout duration to judge that a security server is unreachable, in seconds. The value range is from 1 to 120.

tries *tries-number*: Configures the consecutive timeout count to judge that a security server is unreachable. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

It is judged that a TACACS+ server is unreachable only when both conditions below are met:

- The device fails to receive a correct response packet from the TACACS+ server within the specified timeout period.
- The consecutive transmission count of a request packet sent by the device to the same TACACS+ server reaches the specified timeout count.

Examples

The following example configures the criteria for judging that a TACACS+ server is unreachable as follows: The server timeout duration is **120** seconds and the consecutive timeout count is **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tacacs-server dead-criteria time 120 tries 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 tacacs-server deadtime

Function

Run the **tacacs-server deadtime** command to configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

Run the **no** form of this command to restore the default configuration.

Even if a TACACS+ server is unreachable, the device still sends requests to the TACACS+ server by default.

Syntax

tacacs-server deadtime *deadtime*

no tacacs-server deadtime

Parameter Description

deadtime: Duration for the device to stop sending requests to an unreachable TACACS+ server, in minutes. The value range is from 1 to 1440.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If active detection is enabled for a TACACS+ server on the device, the time parameter configured by the command does not take effect on the TACACS+ server. Otherwise, if the duration in which the TACACS+ server is unreachable exceeds the time specified by the command, the device automatically restores the TACACS+ server to the reachable state.

Examples

The following example sets the duration for the device to stop sending request packets to an unreachable TACACS+ server to **1** minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tacacs-server deadtime 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 IEEE 802.1X Commands

Command	Function
aaa authorization ip-auth-mode	Configure the global IP authorization mode.
clear dot1x user	Delete an IEEE 802.1X-authenticated user on the device.
dot1x accounting	Configure an accounting method list.
dot1x acct-update base-on first-time server	Set the accounting update period to that delivered by the server at the first authentication.
dot1x auth-fail max-attempt	Configure the maximum number of consecutive failed authentication attempts.
dot1x auth-fail vlan	Configure the failed VLAN.
dot1x auth-mode	Configure the authentication mode.
dot1x auth-address-table	Configure a list of hosts allowed for authentication.
dot1x auth-with-order	Set the priority of MAB to be higher than that of IEEE 802.1X authentication.
dot1x authentication	Configure an authentication method list.
dot1x auto-req	Enable the active IEEE 802.1X authentication function on the device.
dot1x auto-req packet-num	Configure the maximum number of active authentication request packets that can be sent by the device.
dot1x auto-req req-interval	Configure the interval for the device to send active authentication request packets.
dot1x auto-req user-detect	Enable the function of detecting whether a user is being authenticated during active authentication.
dot1x client-probe enable	Enable online Ruijie client detection.
dot1x critical	Enable the inaccessible authentication bypass (IAB) function.
dot1x critical recovery action reinitialize	Enable the IAB recovery.
dot1x critical vlan	Configure the IAB VLAN.
dot1x dbg-filter	Configure the debugging of a specific MAC address.

dot1x default-user-limit	Configure the maximum number of users who can be authenticated on an interface.
dot1x default	Restore the default configuration of IEEE 802.1X.
dot1x dynamic-vlan enable	Enable dynamic VLAN redirection on a port.
dot1x guest-vlan	Configure the guest VLAN on a controlled port.
dot1x mab-username upper	Configure usernames used for MAB to use uppercase letters.
dot1x mac-auth-bypass	Enable single-user MAB.
dot1x mac-auth-bypass multi-user	Enable multi-user MAB.
dot1x mac-auth-bypass timeout-activity	Configure the MAB timeout duration.
dot1x mac-auth-bypass violation	Enable the MAB violation function.
dot1x mac-auth-bypass vlan	Configure the MAB VLAN.
dot1x max-req	Configure the maximum retransmission count of Request/Challenge packets.
dot1x multi-account enable	Enable multi-account authentication with one MAC address.
dot1x multi-mab quiet-period	Configure the quiet period after a multi-user MAB failure.
dot1x multi-mab quiet-user fail-times	Configure the number of authentication failures required for user entry aging.
dot1x multi-mab quiet-user authen-num	Configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.
dot1x multi-mab quiet-user reject-times	Configure the server rejection count for the device to delete a quiet user entry.
dot1x mab-username format	Configure the username format for MAB.
dot1x port-control auto	Enable IEEE 802.1X authentication on a port.
dot1x port-control-mode	Configure the port control mode.
dot1x probe-timer interval	Configure the Ruijie client detection interval.
dot1x probe-timer alive	Configure the Ruijie client detection duration.
dot1x private-supplicant-only	Enable the non-Ruijie client filtering function.

dot1x pseudo source-mac	Configure a virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.
dot1x redirect	Enable the 2nd-generation Ruijie Supplicant deployment function.
dot1x reauth-max	Configure the maximum retransmission count of the Request/Identity packets.
dot1x re-authentication	Enable re-authentication.
dot1x stationarity enable	Disable dynamic user migration.
dot1x timeout re-authperiod	Configure the re-authentication interval.
dot1x timeout quiet-period	Configure the quiet period after an authentication failure.
dot1x timeout supp-timeout	Configure the retransmission interval of Request/Challenge packets.
dot1x timeout server-timeout	Configure the server timeout duration.
dot1x timeout tx-period	Configure the retransmission interval of Request/Identity packets.
dot1x user-name compatible	Enable the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.
dot1x valid-ip-acct enable	Enable the function of initiating accounting after a user's IP address is obtained.
dot1x valid-ip-acct timeout	Configure the timeout duration for an authenticated user to obtain an IP address.
dot1x system disable	Disable global IEEE 802.1X features.
show dot1x	Display IEEE 802.1X protocol parameters.
show dot1x auth-address-table	Display the list of hosts allowed for authentication.
show dot1x auto-req	Display active authentication status and parameters.
show dot1x max-req	Display the maximum retransmission count of Request/Challenge packets.
show dot1x port-control	Display information about controlled ports.
show dot1x private-supplicant-only	Display the status of the non-Ruijie client filtering function.
show dot1x probe-timer	Display the client detection parameters.
show dot1x re-authentication	Display the status of the re-authentication function.

show dot1x reauth-max	Display the maximum retransmission count of Request/Identity packets.
show dot1x summary	Display entries of users participating in authentication.
show dot1x timeout quiet-period	Display the quiet period after an authentication failure.
show dot1x timeout re-authperiod	Display the re-authentication interval.
show dot1x timeout server-timeout	Display the server timeout duration.
show dot1x timeout supp-timeout	Display the retransmission interval of Request/Challenge packets.
show dot1x timeout tx-period	Display the retransmission interval of Request/Identity packets.
show dot1x user mac	Display details about a user with a specified MAC address.
show dot1x user name	Display details about a user with a specified username.

1.1 aaa authorization ip-auth-mode

Function

Run the **aaa authorization ip-auth-mode** command to configure the global IP authorization mode.

Run the **no** form of this command to disable this feature.

Global IP authorization is disabled by default.

Syntax

aaa authorization ip-auth-mode { **dhcp-server** | **disable** | **mixed** | **radius-server** | **supplicant** }

no aaa authorization ip-auth-mode

Parameter Description

dhcp-server: Configures the Dynamic Host Configuration Protocol (DHCP) authorization mode, in which IP addresses are assigned via DHCP for binding.

disable: Disables authorization.

mixed: Configures the mixed authorization mode. In the existence of multiple global IP authorization modes, authenticated users select an IP authorization mode based on the sequence of Supplicant authorization, Remote Authentication Dial In User Service (RADIUS) authorization, and DHCP authorization.

radius-server: Configures the RADIUS authorization mode, in which IP addresses are delivered by a RADIUS server for binding.

supplicant: Configures the Supplicant authorization mode, in which Supplicant provides IP addresses for binding.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The Supplicant authorization mode supports only Ruijie Supplicant.

In RADIUS authorization mode, the server needs to deliver IP addresses through the **framed-ip** attribute.

In DHCP authorization mode, DHCP snooping or DHCP relay needs to be enabled on the device.

You are advised to use the mixed authorization mode in the case of multiple authorization modes.

Examples

The following example configures the Supplicant authorization mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authorization ip-auth-mode supplicant
```

Notifications

N/A

Common Errors

IP authorization occupies hardware resources. The considerable number of users in the network and coexistence of multiple security functions may lead to hardware resource insufficiency, which finally causes the failure of users to access the network.

Platform Description

N/A

Related Commands

N/A

1.2 clear dot1x user

Function

Run the **clear dot1x user** command to delete an IEEE 802.1X-authenticated user on the device.

Syntax

clear dot1x user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *user-name* }

Parameter Description

all: Deletes all IEEE 802.1X-authenticated users.

ip *ipv4-address*: Deletes an IEEE 802.1X-authenticated user with a specific IP address.

mac *mac-address*: Deletes an IEEE 802.1X-authenticated user with a specific MAC address.

name *user-name*: Deletes an IEEE 802.1X-authenticated user with a specific username.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example deletes all IEEE 802.1X-authenticated users from the device.

```
Hostname> enable
Hostname# clear dot1x user all
```

The following example deletes an IEEE 802.1X-authenticated user with the IP address 11.1.1.1.

```
Hostname> enable
Hostname# clear dot1x user ip 11.1.1.1
```

The following example deletes an IEEE 802.1X-authenticated user with the MAC address 0012.3456.789A.

```
Hostname> enable
Hostname# clear dot1x user mac 0012.3456.789A
```

The following example deletes an IEEE 802.1X-authenticated user with the username **dot1x-user**.

```
Hostname> enable
Hostname# clear dot1x user name dot1x-user
```

Notifications

N/A

Platform Description

N/A

1.3 dot1x accounting

Function

Run the **dot1x accounting** command to configure an accounting method list.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x accounting { **default |** *list-name* }

no dot1x accounting

Parameter Description

default: Uses the default accounting method list.

list-name: Name of a specified accounting method list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Define a method list in AAA before configuring this command.

Examples

The following example configures an accounting method list named **dot1x-acct**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x accounting dot1x-acct
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **aaa accounting network** (AAA)

1.4 dot1x acct-update base-on first-time server

Function

Run the **dot1x acct-update base-on first-time server** command to set the accounting update period to that delivered by the server at the first authentication.

Run the **no** form of this command to remove this configuration.

The accounting update period delivered by the server at the first authentication is not configured as the accounting update period for re-authentication by default.

Syntax

dot1x acct-update base-on first-time server

no dot1x acct-update base-on first-time server

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Some servers do not deliver the accounting update period during user re-authentication, but require that accounting update packets be sent at the accounting update period delivered at the first authentication. In this case, you can configure this command to meet this requirement.

Examples

The following example sets the accounting update period to that delivered by the server at the first authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x acct-update base-on first-time server
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 dot1x auth-fail max-attempt

Function

Run the **dot1x auth-fail max-attempt** command to configure the maximum number of consecutive failed authentication attempts.

Run the **no** form of this command to restore the default configuration.

The default maximum number of consecutive failed authentication attempts is **3**.

Syntax

dot1x auth-fail max-attempt *max-attempt-number*

no dot1x auth-fail max-attempt

Parameter Description

max-attempt-number: Maximum number of consecutive failed authentication attempts. The value range is from 1 to 3.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of times that a user is consecutively rejected by the authentication server. If the rejection count reaches this number, the port, to which the user is connected, will be added to a failed VLAN and the user is allowed to access network resources in the failed VLAN.

Examples

The following example sets the maximum number of consecutive failed authentication attempts to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-fail max-attempt 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auth-fail vlan**

1.6 dot1x auth-fail vlan

Function

Run the **dot1x auth-fail vlan** command to configure the failed VLAN.

Run the **no** form of this command to disable this feature.

The failed VLAN function is disabled by default.

Syntax

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

Parameter Description

vlan-id: VLAN, to which users who fail the authentication are to be added. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the failed VLAN is configured, users who fail the authentication can access network resources only in the failed VLAN.

Examples

The following example sets the failed VLAN to VLAN 30.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x auth-fail vlan 30
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auth-fail max-attempt**

1.7 dot1x auth-mode

Function

Run the **dot1x auth-mode** command to configure the authentication mode.

Run the **no** form of this command to restore the default configuration.

The default authentication mode is Extensible Authentication Protocol (EAP) mode.

Syntax

dot1x auth-mode { **chap** | **eap** | **pap** }

no dot1x auth-mode

Parameter Description

chap: Sets the authentication mode to Challenge-Handshake Authentication Protocol (CHAP) mode.

eap: Sets the authentication mode to EAP mode.

pap: Sets the authentication mode to Password Authentication Protocol (PAP) mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Select an authentication mode based on whether Ruijie Supplicant is supported and the authentication mode supported by the authentication server.

Examples

The following example sets the authentication mode to CHAP mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-mode chap
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.8 dot1x auth-address-table

Function

Run the **dot1x auth-address-table** command to configure a list of hosts allowed for authentication.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

no dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

Parameter Description

mac-address: MAC address of an access client allowed for authentication.

interface-type interface-number: Interface type and interface number of the access client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to allow only clients with specific MAC addresses on a specified port to perform IEEE 802.1X authentication.

Examples

The following example sets the access port of a host allowed for authentication to GigabitEthernet 0/1 and the MAC address to 00d0.f800.0cb2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-address-table address 00d0.f800.0cb2 interface
gigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

1.9 dot1x auth-with-order

Function

Run the **dot1x auth-with-order** command to set the priority of MAB to be higher than that of IEEE 802.1X authentication.

Run the **no** form of this command to restore the default configuration.

The priority of MAB is lower than that of IEEE 802.1X authentication by default.

Syntax

dot1x auth-with-order

no dot1x auth-with-order

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The priority of IEEE 802.1X authentication is higher than that of MAB by default. If IEEE 802.1X authentication is performed after MAB is completed, the IEEE 802.1X authentication result will replace the MAB result. After this function is enabled, MAB has a higher priority and the device performs MAB first. The IEEE 802.1X authentication result cannot replace the MAB result.

Examples

The following example sets the priority of MAB to be higher than that of IEEE 802.1X authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x auth-with-order
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 dot1x authentication

Function

Run the **dot1x authentication** command to configure an authentication method list.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x authentication { **default** | *list-name* }

no dot1x authentication

Parameter Description

default: Uses the default authentication method list.

list-name: Name of a specified authentication method list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Define a method list in AAA before configuring this command.

Examples

The following example configures an authentication method list named **dot1x-authen**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x authentication dot1x-authen
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **aaa authentication dot1x** (AAA)

1.11 dot1x auto-req

Function

Run the **dot1x auto-req** command to enable the active IEEE 802.1X authentication function on the device.

Run the **no** form of this command to disable this feature.

The active IEEE 802.1X authentication function is enabled by default.

Syntax

dot1x auto-req

no dot1x auto-req

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Active authentication refers that the device actively sends a Request/Identity packet, which triggers IEEE 802.1X clients to initiate IEEE 802.1X authentication.

This function must be enabled for MAB deployment.

Some clients use authentication clients embedded in the operating system (OS). They may not initiate authentication immediately after connecting to the network, and users cannot use the network promptly. The

configured active authentication can urge such clients to initiate authentication in a timely manner after they connect to the network.

Do not enable this function when a controlled port is a trunk port and is directly connected to clients. Otherwise, frequent authentication or going offline may occur.

Examples

The following example enables active 802.1X authentication on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auto-req
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 dot1x auto-req packet-num

Function

Run the **dot1x auto-req packet-num** command to configure the maximum number of active authentication request packets that can be sent by the device.

Run the **no** form of this command to restore the default configuration.

The device always sends authentication request packets actively by default.

Syntax

dot1x auto-req packet-num *packet-number*

no dot1x auto-req packet-num

Parameter Description

packet-number: Maximum number of active authentication request packets that can be sent. The value range is from 0 to 1000000 and the value **0** indicates that the device sends authentication request packets continuously.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of active authentication request packets that can be sent by the device to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auto-req packet-num 100
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auto-req**

1.13 dot1x auto-req req-interval

Function

Run the **dot1x auto-req req-interval** command to configure the interval for the device to send active authentication request packets.

Run the **no** form of this command to restore the default configuration.

The default interval for the device to send active authentication request packets is **30** seconds.

Syntax

dot1x auto-req req-interval *req-interval*

no dot1x auto-req req-interval

Parameter Description

req-interval: Interval for sending active authentication request packets, in seconds. The value range is from 10 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for the device to send active authentication request packets to 50 seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# dot1x auto-req req-interval 50
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auto-req**

1.14 dot1x auto-req user-detect

Function

Run the **dot1x auto-req user-detect** command to enable the function of detecting whether a user is being authenticated during active authentication.

Run the **no** form of this command to disable this feature.

The function of detecting whether a user is being authenticated during active authentication is enabled by default.

Syntax

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to enable this function only when one client is connected to a port, to reduce authentication load of the server.

Examples

The following example disables the function of detecting whether a user is being authenticated during active authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no dot1x auto-req user-detect
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 dot1x client-probe enable

Function

Run the **dot1x client-probe enable** command to enable online Ruijie client detection.

Run the **no** form of this command to disable this feature.

Online Ruijie client detection is disabled by default.

Syntax

dot1x client-probe enable

no dot1x client-probe enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to enable this function when Ruijie Supplicant is used.

Examples

The following example enables online Ruijie client detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x client-probe enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 dot1x critical

Function

Run the **dot1x critical** command to enable the inaccessible authentication bypass (IAB) function.

Run the **no** form of this command to disable this feature.

IAB is disabled by default.

Syntax

dot1x critical

no dot1x critical

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

IAB is a method provided for new to-be-authenticated users to access the network when all RADIUS servers configured on the device are all unreachable. After a RADIUS server becomes reachable, it verifies the identities of users authorized in the unavailability period of RADIUS servers.

Examples

The following example enables IAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 dot1x critical recovery action reinitialize

Function

Run the **dot1x critical recovery action reinitialize** command to enable the IAB recovery.

Run the **no** form of this command to disable this feature.

IAB recovery is disabled by default.

Syntax

dot1x critical recovery action reinitialize

no dot1x critical recovery action reinitialize

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, if a RADIUS server becomes reachable, it verifies the identities of users authorized by IAB in the unavailability period of RADIUS servers.

Examples

The following example enables IAB recovery.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical recovery action reinitialize
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.18 dot1x critical vlan

Function

Run the **dot1x critical vlan** command to configure the IAB VLAN.

Run the **no** form of this command to disable this feature.

The IAB VLAN function is disabled by default.

Syntax

dot1x critical vlan *vlan-id*

no dot1x critical vlan

Parameter Description

vlan-id: ID of an IAB VLAN. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IAB VLAN to VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical vlan 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x critical**

1.19 dot1x dbg-filter

Function

Run the **dot1x dbg-filter** command to configure the debugging of a specific MAC address.

Run the **no** form of this command to remove this configuration.

Debugging information of all authenticated users is printed by default.

Syntax

dot1x dbg-filter *mac-address*

no dot1x dbg-filter *mac-address*

Parameter Description

mac-address: MAC address of a user whose debugging information needs to be output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When there are a large number of users in the network and a network fault needs to be pinpointed, you can configure the debugging of users with specific MAC addresses, to avoid outputting debugging information of too many irrelevant users.

Examples

The following example debugs the MAC address 00d0.f800.0001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x dbg-filter 00d0.f800.0001
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 dot1x default-user-limit

Function

Run the **dot1x default-user-limit** command to configure the maximum number of users who can be authenticated on an interface.

Run the **no** form of this command to restore the default configuration.

The maximum number of users who can be authenticated on an interface is unlimited.

Syntax

dot1x default-user-limit *limit-number*

no dot1x default-user-limit

Parameter Description

limit-number: Maximum number of users who can be authenticated on an interface. The value range is from 1 to 1000000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of users who can be authenticated on an interface to 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x default-user-limit 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 dot1x default

Function

Run the **dot1x default** command to restore the default configuration of IEEE 802.1X.

Syntax

dot1x default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can clear existing IEEE 802.1X configurations in one-click mode. Use this command when considerable 802.1X configurations need to be cleared and reconfiguration is needed.

Examples

The following example restores the default configuration of IEEE 802.1X.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x default
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 dot1x dynamic-vlan enable

Function

Run the **dot1x dynamic-vlan enable** command to enable dynamic VLAN redirection on a port.

Run the **no** form of this command to disable this feature.

Dynamic VLAN redirection is disabled on a port by default.

Syntax

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configure this command when authenticated users need to be added to the VLAN delivered by the server.

Examples

The following example enables dynamic VLAN redirection on a port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 dot1x guest-vlan

Function

Run the **dot1x guest-vlan** command to configure the guest VLAN on a controlled port.

Run the **no** form of this command to disable this feature.

The guest VLAN function is disabled on a controlled port by default.

Syntax

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Parameter Description

vlan-id: Guest VLAN, to which a port needs to be added. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The guest VLAN function is used to provide network access permissions for terminals, on which the IEEE 802.1X client is not installed.

After the guest VLAN function is configured, if no IEEE 802.1X client is detected on a controlled port, the port is added to the guest VLAN to allow terminals connected to the port to access network resources in the guest VLAN.

After guest VLAN is enabled on a port, do not configure L2 attributes, especially do not manually configure the port VLAN.

Examples

The following example sets the guest VLAN to VLAN 20 on a controlled port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x guest-vlan 20
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x dynamic-vlan enable**

1.24 dot1x mab-username upper

Function

Run the **dot1x mab-username upper** command to configure usernames used for MAB to use uppercase letters.

Run the **no** form of this command to restore the default configuration.

Usernames used for MAB use lowercase letters by default.

Syntax

dot1x mab-username upper

no dot1x mab-username upper

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to meet requirements of different servers for username uppercase/lowercase in MAB.

Examples

The following example configures usernames used for MAB to use uppercase letters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x mab-username upper
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.25 dot1x mac-auth-bypass

Function

Run the **dot1x mac-auth-bypass** command to enable single-user MAB.

Run the **no** form of this command to disable this feature.

Single-user MAB is disabled by default.

Syntax

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Single-user MAB applies to the scenario, in which a port has only one dumb terminal attached to it or a port has only one dumb terminal to be authenticated. After successful authentication, other terminals connected to the port can access the network.

Examples

The following example enables single-user MAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 dot1x mac-auth-bypass multi-user

Function

Run the **dot1x mac-auth-bypass multi-user** command to enable multi-user MAB.

Run the **no** form of this command to disable this feature.

Multi-user MAB is disabled by default.

Syntax

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Multi-user MAB applies when multiple dumb terminals are connected to one port. Multi-user MAB can be used together with IEEE 802.1X authentication in mixed access scenarios such as the PC+VoIP daisy-chain topology.

Examples

The following example enables multi-user MAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass multi-user
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 dot1x mac-auth-bypass timeout-activity

Function

Run the **dot1x mac-auth-bypass timeout-activity** command to configure the MAB timeout duration.

Run the **no** form of this command to remove this configuration.

MAB does not time out by default.

Syntax

dot1x mac-auth-bypass timeout-activity *timeout*

no dot1x mac-auth-bypass timeout-activity

Parameter Description

timeout: MAB timeout duration, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can configure this parameter to restrict the network access duration of dumb terminals.

Examples

The following example sets the MAB timeout duration to 3,600 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass timeout-activity 3600
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 dot1x mac-auth-bypass violation

Function

Run the **dot1x mac-auth-bypass violation** command to enable the MAB violation function.

Run the **no** form of this command to disable this feature.

MAB violation is disabled by default.

Syntax

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This function can be configured to restrict one port to have only one dumb terminal. This command applies only to single-user MAB scenarios.

Examples

The following example enables the MAB violation function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass violation
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 dot1x mac-auth-bypass vlan

Function

Run the **dot1x mac-auth-bypass vlan** command to configure the MAB VLAN.

Run the **no** form of this command to disable this feature.

The MAB VLAN function is disabled by default.

Syntax

dot1x mac-auth-bypass vlan *vlan-id*

no dot1x mac-auth-bypass vlan *vlan-id*

Parameter Description

vlan-id: ID of a VLAN allowed for MAB. The value is a valid VLAN ID. If you configure multiple VLAN IDs, separate them with commas (,). You can also configure a VLAN ID range, for example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured to only allow users in a specific VLAN on an interface to perform MAB.

Examples

The following example sets MAB VLANs to VLAN 5 and VLANs 8-20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass vlan 5, 8-20
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 dot1x max-req

Function

Run the **dot1x max-req** command to configure the maximum retransmission count of Request/Challenge packets.

Run the **no** form of this command to restore the default configuration.

The default maximum retransmission count of Request/Challenge packets is **3**.

Syntax

dot1x max-req *max-req-number*

no dot1x max-req

Parameter Description

max-req-number: Maximum retransmission count of Request/Challenge packets. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the maximum retransmission count of Request/Challenge packets to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x max-req 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.31 dot1x multi-account enable

Function

Run the **dot1x multi-account enable** command to enable multi-account authentication with one MAC address.

Run the **no** form of this command to disable this feature.

Multi-account authentication with one MAC address is disabled by default.

Syntax

dot1x multi-account enable

no dot1x multi-account enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to handle account switching during authentication or re-authentication, for example, domain authentication in Windows.

Examples

The following example enables multi-account authentication with one MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-account enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.32 dot1x multi-mab quiet-period

Function

Run the **dot1x multi-mab quiet-period** command to configure the quiet period after a multi-user MAB failure.

Run the **no** form of this command to restore the default configuration.

The default quiet period after a multi-user MAB failure is **30** seconds.

Syntax

dot1x multi-mab quiet-period *quiet-period*

no dot1x multi-mab quiet-period

Parameter Description

quiet-period: Quiet period after a multi-user MAB failure, in seconds. The value range is from 0 to 65535 and the value **0** indicates no quiet period.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After multi-user MAB is enabled, illegitimate users connected to an interface may attack the device. Therefore, it is necessary to prevent illegitimate users from frequently initiating authentication, in an effort to reduce the server load. Configure the quiet period after a multi-user MAB failure in global configuration mode. After configuration, if a MAC address fails the authentication, it can re-initiate authentication only after the quiet period elapses. Configure this quiet period as required.

Examples

The following example sets the quiet period after a multi-user MAB failure to 2 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-period 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.33 dot1x multi-mab quiet-user fail-times

Function

Run the **dot1x multi-mab quiet-user fail-times** command to configure the number of authentication failures required for user entry aging.

Run the **no** form of this command to restore the default configuration.

The default number of authentication failures required for user entry aging is **60**.

Syntax

dot1x multi-mab quiet-user fail-times [*fail-times*]

no dot1x multi-mab quiet-user fail-times

Parameter Description

fail-times: Number of authentication failures required for user entry aging. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure aging rules for users who fail the authentication.

Examples

The following example sets the number of authentication failures required for user entry aging to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user fail-times 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.34 dot1x multi-mab quiet-user authen-num

Function

Run the **dot1x multi-mab quiet-user authen-num** command to configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.

Run the **no** form of this command to restore the default configuration.

The default rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry is **50** MAC addresses per second.

Syntax

dot1x multi-mab quiet-user authen-num [*authen-num*]

no dot1x multi-mab quiet-user authen-num

Parameter Description

authen-num: Rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry, in MAC addresses per second. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry to 3 MAC addresses per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user authen-num 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.35 dot1x multi-mab quiet-user reject-times

Function

Run the **dot1x multi-mab quiet-user reject-times** command to configure the server rejection count for the device to delete a quiet user entry.

Run the **no** form of this command to restore the default configuration.

The default server rejection count for the device to delete a quiet user entry is **1**.

Syntax

dot1x multi-mab quiet-user reject-times [*reject-times*]

no dot1x multi-mab quiet-user reject-times

Parameter Description

reject-times: Server rejection count for the device to delete a quiet user entry.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the device to delete a quiet user entry after the server rejects the user authentication three times.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user reject-times 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.36 dot1x mab-username format

Function

Run the **dot1x mab-username format** command to configure the username format for MAB.

Run the **no** form of this command to remove this configuration.

No username format for MAB is configured by default.

Syntax

dot1x mab-username format [**with-colon** | **with-dot** | **with-hyphen** | **with-3hyphen**]

no dot1x mab-username format

Parameter Description

with-colon: Indicates that the username format is xx:xx:xx:xx:xx:xx.

with-dot: Indicates that the username format is xxxx.xxxx.xxxx.

with-hyphen: Indicates that the username format is xx-xx-xx-xx-xx-xx.

with-3hyphen: Indicates that the username format is xxxx-xxxx-xxxx.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the required username format for MAB is xx-xx-xx-xx-xx-xx, configure **with-hyphen** in this command.

When the required username format for MAB is xxxx.xxxx.xxxx, configure **with-dot** in this command.

When the required username format for MAB is xx:xx:xx:xx:xx:xx, configure **with-colon** in this command.

When the required username format for MAB is xxxx-xxxx-xxxx, configure **with-3hyphen** in this command.

Examples

The following example sets the username format for MAB to **with-hyphen**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x mab-username format with-hyphen
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.37 dot1x port-control auto

Function

Run the **dot1x port-control auto** command to enable IEEE 802.1X authentication on a port.

Run the **no** form of this command to disable this feature.

IEEE 802.1X authentication is disabled on a port by default.

Syntax

dot1x port-control auto

no dot1x port-control auto

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Other IEEE 802.1X commands are meaningful only after this command is configured.

Examples

The following example enables IEEE 802.1X authentication on a port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x port-control auto
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.38 dot1x port-control-mode

Function

Run the **dot1x port-control-mode** command to configure the port control mode.

Run the **no** form of this command to restore the default configuration.

The default port control mode is MAC-based control.

Syntax

dot1x port-control-mode { **mac-based** | **port-based** [**single-host**] }

no dot1x port-control-mode

Parameter Description

mac-based: Sets the port control mode to MAC-based control.

port-based [**single-host**]: Sets the port control mode to port-based control. **single-host** indicates that only one client is allowed on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configure the MAC-based control mode if each user on a controlled port has to pass authentication before making communication.

Configure the port-based control mode if all users on a controlled port can make communication after one of them passes the authentication.

In port-based control mode, this command can be configured only when authenticated users are dynamic users.

Examples

The following example sets the port control mode to port-based control.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x port-control-mode port-based
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.39 dot1x probe-timer interval

Function

Run the **dot1x probe-timer interval** command to configure the Ruijie client detection interval.

Run the **no** form of this command to restore the default configuration.

The default client detection interval is **20** seconds.

Syntax

dot1x probe-timer interval *interval*

no dot1x probe-timer interval

Parameter Description

interval: Client detection interval, in seconds. The value range is from 1 to 32767.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default configuration is recommended.

The interval for sending packets to detect whether Ruijie clients are online must be smaller than half of the online detection duration.

Examples

The following example sets the Ruijie client detection interval to 30 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x probe-timer interval 30
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x probe-timer alive**

1.40 dot1x probe-timer alive

Function

Run the **dot1x probe-timer alive** command to configure the Ruijie client detection duration.

Run the **no** form of this command to restore the default configuration.

The default Ruijie client detection duration is **250** seconds.

Syntax

dot1x probe-timer alive *alive-time*

no dot1x probe-timer alive

Parameter Description

alive-time: Ruijie client detection duration, in seconds. The value range is from 3 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After a client is authenticated and goes online, if the device fails to receive any detection response from the client within the detection duration, the device considers the client offline.

The default configuration is recommended.

The online detection duration must be greater than twice the interval for sending packets to detect whether Ruijie clients are online.

Examples

The following example sets the Ruijie client detection duration to 120 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x probe-timer alive 120
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x probe-timer interval**

1.41 dot1x private-supplicant-only

Function

Run the **dot1x private-supplicant-only** command to enable the non-Ruijie client filtering function.

Run the **no** form of this command to disable this feature.

The non-Ruijie client filtering function is disabled by default.

Syntax

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This function should be configured if Ruijie Supplicant must be used for authentication.

Examples

The following example enables the non-Ruijie client filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x private-supplicant-only
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 dot1x pseudo source-mac

Function

Run the **dot1x pseudo source-mac** command to configure a virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.

Run the **no** form of this command to remove this configuration.

The source MAC address of IEEE 802.1X packets sent by the device is a virtual MAC address by default.

Syntax

dot1x pseudo source-mac

no dot1x pseudo source-mac

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Some Ruijie Supplicant versions judge whether an access device is a Ruijie device based on the source MAC addresses of EAP packets, so as to implement Ruijie private features. If a device works with such Supplicant versions to perform IEEE 802.1X authentication and private features are needed, configure this command on the device.

Examples

The following example configures not to use the virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no dot1x pseudo source-mac
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 dot1x redirect

Function

Run the **dot1x redirect** command to enable the 2nd-generation Ruijie Supplicant deployment function.

Run the **no** form of this command to disable this feature.

The 2nd-generation Ruijie Supplicant deployment function is disabled by default.

Syntax

dot1x redirect

no dot1x redirect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The 2nd-generation Ruijie Supplicant deployment function redirects the browser to a specified resource website so that the Supplicant software can be downloaded.

Redirection parameters need to be configured.

Examples

The following example enables the 2nd-generation Ruijie Supplicant deployment function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x redirect
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

Related Commands

N/A

1.44 dot1x reauth-max

Function

Run the **dot1x reauth-max** command to configure the maximum retransmission count of the Request/Identity packets.

Run the **no** form of this command to restore the default configuration.

The default maximum retransmission count of Request/Identity packets is **3**.

Syntax

dot1x reauth-max *reauth-max-number*

no dot1x reauth-max

Parameter Description

reauth-max-number: Maximum retransmission count of Request/Identity packets. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the maximum retransmission count of Request/Identity packets to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x reauth-max 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 dot1x re-authentication

Function

Run the **dot1x re-authentication** command to enable re-authentication.

Run the **no** form of this command to disable this feature.

The re-authentication function is disabled by default.

Syntax

dot1x re-authentication

no dot1x re-authentication

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Re-authentication brings great burden to the server. You are advised to disable this function in an environment with a large number of users.

Examples

The following example enables the re-authentication function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x re-authentication
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 dot1x stationarity enable

Function

Run the **dot1x stationarity enable** command to disable dynamic user migration.

Run the **no** form of this command to restore the default configuration.

Dynamic user migration is enabled by default.

Syntax

dot1x stationarity enable

no dot1x stationarity enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, dynamic users are not allowed to migrate to other ports in port-based control mode.

Examples

The following example disables dynamic user migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x stationarity enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 dot1x timeout re-authperiod

Function

Run the **dot1x timeout re-authperiod** command to configure the re-authentication interval.

Run the **no** form of this command to restore the default configuration.

The default re-authentication interval is **3600** seconds.

Syntax

dot1x timeout re-authperiod *interval*

no dot1x timeout re-authperiod

Parameter Description

interval: Re-authentication interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the re-authentication interval to 2,400 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout re-authperiod 2400
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x re-authentication**

1.48 dot1x timeout quiet-period

Function

Run the **dot1x timeout quiet-period** command to configure the quiet period after an authentication failure.

Run the **no** form of this command to restore the default configuration.

The default quiet period after an authentication failure is **10** seconds.

Syntax

dot1x timeout quiet-period *quiet-period*

no dot1x timeout quiet-period

Parameter Description

quiet-period: Quiet period after an authentication failure, in seconds. The value range is from 0 to 65535 and the value **0** indicates no quiet period.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the quiet period after an authentication failure to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout quiet-period 60
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 dot1x timeout supp-timeout

Function

Run the **dot1x timeout supp-timeout** command to configure the retransmission interval of Request/Challenge packets.

Run the **no** form of this command to restore the default configuration.

The default retransmission interval of Request/Challenge packets is **3** seconds.

Syntax

dot1x timeout supp-timeout *interval*

no dot1x timeout supp-timeout

Parameter Description

interval: Retransmission interval of Request/Challenge packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the retransmission interval of Request/Challenge packets to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout supp-timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.50 dot1x timeout server-timeout

Function

Run the **dot1x timeout server-timeout** command to configure the server timeout duration.

Run the **no** form of this command to restore the default configuration.

The default server timeout duration is **5** seconds.

Syntax

dot1x timeout server-timeout *server-timeout*

no dot1x timeout server-timeout

Parameter Description

server-timeout: Server timeout time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The server timeout duration of IEEE 802.1X must be greater than that of RADIUS.

The server timeout duration of IEEE 802.1X is smaller than that of RADIUS by default. Set the server timeout duration of RADIUS to a smaller value in actual application.

Examples

The following example sets the server timeout duration to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout server-timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 dot1x timeout tx-period

Function

Run the **dot1x timeout tx-period** command to configure the retransmission interval of Request/Identity packets.

Run the **no** form of this command to restore the default configuration.

The default retransmission interval of Request/Identity packets is **3** seconds.

Syntax

dot1x timeout tx-period *interval*

no dot1x timeout tx-period

Parameter Description

interval: Retransmission interval of Request/Identity packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the retransmission interval of Request/Identity packets to 5 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout tx-period 5
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 dot1x user-name compatible

Function

Run the **dot1x user-name compatible** command to enable the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.

Run the **no** form of this command to disable this feature.

The compatibility with H3C 802.1X authentication clients and authentication servers is disabled by default.

Syntax

dot1x user-name compatible

no dot1x user-name compatible

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Configure this command when H3C authentication clients and authentication servers are used for IEEE 802.1X authentication.

Configure this command when H3C authentication servers are used for MAB.

Examples

The following example enables the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x user-name compatible
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.53 dot1x valid-ip-acct enable

Function

Run the **dot1x valid-ip-acct enable** command to enable the function of initiating accounting after a user's IP address is obtained.

Run the **no** form of this command to disable this feature.

The function of initiating accounting after a user's IP address is obtained is disabled by default.

Syntax

dot1x valid-ip-acct enable

no dot1x valid-ip-acct enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, clients do not initiate accounting immediately after passing authentication, but wait until they obtain IP addresses.

Configure this function when a server requires that accounting packets carry user IP addresses.

Examples

The following example enables the function of initiating accounting after a user's IP address is obtained.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x valid-ip-acct enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.54 dot1x valid-ip-acct timeout

Function

Run the **dot1x valid-ip-acct timeout** command to configure the timeout duration for an authenticated user to obtain an IP address.

Run the **no** form of this command to restore the default configuration.

The default timeout duration for an authenticated user to obtain an IP address is **5** minutes.

Syntax

dot1x valid-ip-acct timeout *timeout*

no dot1x valid-ip-acct timeout

Parameter Description

timeout: Allowed timeout duration for an authenticated user to obtain an IP address, in minutes. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the function of initiating accounting after a user's IP address is obtained, is enabled, a client may not initiate accounting within a long period of time due to the failure to obtain an IP address. For this, you can configure a timeout duration as required.

Examples

The following example sets the timeout duration for an authenticated user to obtain an IP address to 10 minutes.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# dot1x valid-ip-acct timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x valid-ip-acct enable**

1.55 dot1x system disable

Function

Run the **dot1x system disable** command to disable global IEEE 802.1X features.

Run the **no** form of this command to restore the default configuration.

Global IEEE 802.1X features are enabled by default.

Syntax

dot1x system disable

no dot1x system disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Disable global IEEE 802.1X features when servers are unavailable. After global IEEE 802.1X features are disabled, users can access the Internet without authentication and authenticated users will be brought offline.

If global IEEE 802.1X features are enabled after server recovery, users on the controlled ports need to be authenticated before accessing the Internet.

Examples

The following example disables global IEEE 802.1X features.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x system disable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.56 show dot1x

Function

Run the **show dot1x** command to display IEEE 802.1X protocol parameters.

Syntax

show dot1x

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IEEE 802.1X protocol parameters.

```
Hostname> enable
Hostname# show dot1x
802.1X basic information:
  802.1X Status ......................... enable
  Authentication Mode ................... eap
  Authorization mode .................... disable
  Total User Number ..................... 0 (exclude dynamic user)
  Authenticated User Number ............. 0 (exclude dynamic user)
  Dynamic User Number ................... 0
  Re-authentication ..................... disable
  Re-authentication Period .............. 3600 seconds
  Re-authentication max ................. 3 times
  Quiet Period .......................... 10 seconds
  Tx Period ............................. 30 seconds
  Supplicant Timeout .................... 3 seconds
  Server Timeout ........................ 5 seconds
  Maximum Request ....................... 3 times
  Client Online Probe ................... disable
```

```
Eapol Tag ............................ enable
802.1x redirect ...................... disable
Private supplicant only ............... disable
```

Table 1-1 Output Fields of the show dot1x Command

Field	Description
802.1X Status	Whether the IEEE 802.1X function is enabled
Authentication Mode	Authorization mode
Total User Number	Total number of authenticated users and users being authenticated
Authed User Number	Number of authenticated users
Dynamic User Number	Number of dynamic users in port mode
Re-authentication	Status of the re-authentication function
Re-authentication Period	Re-authentication period
Re-authentication max	Maximum number of re-authentication times
Quiet Period	Quiet period after an authentication failure
Tx Period	Retransmission interval of Request/Identity packets
Supplicant Timeout	Retransmission interval of Request/Challenge packets
Server Timeout	Server timeout duration
Maximum Request	Maximum request count
Client Online Probe	Status of online client detection
Eapol Tag	Whether EAPOL packets carry tags
802.1x redirect	Status of the 2nd-generation Ruijie Supplicant deployment function
Private supplicant only	Status of private client detection

Notifications

N/A

Platform Description

N/A

1.57 show dot1x auth-address-table

Function

Run the **show dot1x auth-address-table** command to display the list of hosts allowed for authentication.

Syntax

show dot1x auth-address-table [**address** *mac-address*] [**interface** *interface-type interface-number*]

Parameter Description

address *mac-address*: Specifies the MAC address of a client.

interface *interface-type interface-number*: Specifies the interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the list of hosts allowed for authentication.

```
Hostname> enable
Hostname# show dot1x auth-address-table
Interface       Address
---------------- -------------------
Gi0/1           00d0.f800.0c0e
Gi0/2           001a.c800.0102
Hostname# show dot1x auth-address-table interface fastEthernet 0/1
Interface       Address
---------------- -------------------
Gi0/1           00d0.f800.0c0e
Hostname# show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface       Address
---------------- -------------------
Gi0/1           00d0.f800.0c0e
```

Table 1-2 Output Fields of the show dot1x auth-address-table Command

Field	Description
Interface	Port
Address	MAC address of a host allowed for authentication

Notifications

N/A

Platform Description

N/A

1.58 show dot1x auto-req

Function

Run the **show dot1x auto-req** command to display active authentication status and parameters.

Syntax

show dot1x auto-req

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the active authentication status and parameters.

```
Hostname> enable
Hostname# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
```

Table 1-3 Output Fields of the show dot1x auto-req Command

Field	Description
Auto-Req	Status of the active authentication function
User-Detect	Status of the user detection function
Packet-Num	Number of active authentication request packets
Req-Interval	Transmission interval of active authentication packets

Notifications

N/A

Platform Description

N/A

1.59 show dot1x max-req

Function

Run the **show dot1x max-req** command to display the maximum retransmission count of Request/Challenge packets.

Syntax

show dot1x max-req

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the maximum retransmission count of Request/Challenge packets.

```
Hostname> enable
Hostname# show dot1x max-req
Max-Req: 3 Times
```

Table 1-4 Output Fields of the show dot1x max-req Command

Field	Description
Max-Req	Maximum retransmission count of Request/Challenge packets

Notifications

N/A

Platform Description

N/A

1.60 show dot1x port-control

Function

Run the **show dot1x port-control** command to display information about controlled ports.

Syntax

show dot1x port-control [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and interface number. Information about all controlled ports is displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about controlled ports.

```
Hostname> enable
Hostname# show dot1x port-control
Interface     Mode      Dynamic-User Static-User Max-User  Authened MAB
------------- ---------- ------------ ----------- --------- -------- ---------
Gi0/5    mac-based  0          0         unlimited no      disable
```

Table 1-5 Output Fields of show dot1x port-control Command

Field	Description
Interface	Name of a controlled port
Mode	Port mode
Dynamic-User	Number of dynamic users on the port
Static-User	Number of static users on the port
Max-User	Maximum number of users supported by the port
Authened	Whether the port passes authentication
MAB	Status of MAB configured on the port

Notifications

N/A

Platform Description

N/A

1.61 show dot1x private-supplicant-only

Function

Run the **show dot1x private-supplicant-only** command to display the status of the non-Ruijie client filtering function.

Syntax

show dot1x private-supplicant-only

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the status of the non-Ruijie client filtering function.

```
Hostname> enable
Hostname# show dot1x private-supplicant-only
private-supplicant-only: Disabled
```

Table 1-6 Output Fields of the show dot1x private-supplicant-only Command

Field	Description
private-supplicant-only	Status of the non-Ruijie client filtering function

Notifications

N/A

Platform Description

N/A

1.62 show dot1x probe-timer

Function

Run the **show dot1x probe-timer** command to display the client detection parameters.

Syntax

show dot1x probe-timer

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays client detection parameters.

```
Hostname> enable
Hostname# show dot1x probe-timer
Hello Interval   : 20
Hello Alive      : 60
```

Table 1-7 Output Fields of the show dot1x probe-timer Command

Field	Description
Hello Interval	Detection interval
Hello Alive	Detection duration

Notifications

N/A

Platform Description

N/A

1.63 show dot1x re-authentication

Function

Run the **show dot1x re-authentication** command to display the status of the re-authentication function.

Syntax

show dot1x re-authentication

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the status of the re-authentication function.

```
Hostname> enable
Hostname# show dot1x re-authentication
Reauth-Enabled: Disabled
```

Table 1-8 Output Fields of the show dot1x re-authentication Command

Field	Description
Reauth-Enabled	Status of the re-authentication function

Notifications

N/A

Platform Description

N/A

1.64 show dot1x reauth-max

Function

Run the **show dot1x reauth-max** Command to display the maximum retransmission count of Request/Identity packets.

Syntax

show dot1x reauth-max

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the maximum retransmission count of Request/Identity packets.

```
Hostname> enable
Hostname# show dot1x reauth-max
Reauth-Max: 3 Times
```

Table 1-9 Output Fields of the show dot1x reauth-max Command

Field	Description
Reauth-Max	Maximum retransmission count of Request/Identity packets

Notifications

N/A

Platform Description

N/A

1.65 show dot1x summary

Function

Run the **show dot1x summary** command to display entries of users participating in authentication.

Syntax

show dot1x summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can check user entries to figure out the current phase of a client (for example, being authenticated, authenticated, or quiet).

Examples

The following example displays entries of users participating in authentication.

```
Hostname> enable
Hostname# show dot1x summary
ID       Username                    MAC           Interface VLAN Auth-State
Backend-state Port-Status User-Type Time
-------- ------------------------------ -------------- --------- ----
-------------- ------------ ----------- --------- -----------------
```

Table 1-10 Output Fields of the show dot1x summary Command

Field	Description
ID	ID obtained from AAA (You can run the **show aaa user all** command to check the ID.)
User	Username
MAC	MAC address of a client participating in authentication
Interface	Port, to which the client participating in authentication is connected
VLAN	ID of the VLAN, to which the client participating in authentication belongs
INNER-VLAN	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Auth-State	Status of the authentication state machine
Backend-State	Status of the backend authentication state machine
Port-State	Port authentication status
User-Type	Authentication type
Time	Online duration

Notifications

N/A

Platform Description

N/A

Related Commands

- **show aaa user** (AAA)

1.66 show dot1x timeout quiet-period

Function

Run the **show dot1x timeout quiet-period** command to display the quiet period after an authentication failure.

Syntax

show dot1x timeout quiet-period

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the quiet period after an authentication failure.

```
Hostname> enable
Hostname# show dot1x timeout quiet-period
Quiet-Period: 10 Seconds
```

Table 1-11 Output Fields of the show dot1x timeout quiet-period Command

Field	Description
Quiet-Period	Quiet period after an authentication failure

Notifications

N/A

Platform Description

N/A

1.67 show dot1x timeout re-authperiod

Function

Run the **show dot1x timeout re-authperiod** command to display the re-authentication interval.

Syntax

show dot1x timeout re-authperiod

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the re-authentication interval.

```
Hostname> enable
Hostname# show dot1x timeout re-authperiod
Reauth-Period: 3600 Seconds
```

Table 1-12 Output Fields of the show dot1x timeout re-authperiod Command

Field	Description
Reauth-Period	Re-authentication interval

Notifications

N/A

Platform Description

N/A

1.68 show dot1x timeout server-timeout

Function

Run the **show dot1x timeout server-timeout** command to display the server timeout duration.

Syntax

show dot1x timeout server-timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the server timeout duration.

```
Hostname> enable
Hostname# show dot1x timeout server-timeout
Server-Timeout: 5 Seconds
```

Table 1-13 Output Fields of the show dot1x timeout server-timeout Command

Field	Description
Server-Period	Server timeout duration

Notifications

N/A

Platform Description

N/A

1.69 show dot1x timeout supp-timeout

Function

Run the **show dot1x timeout supp-timeout** command to display the retransmission interval of Request/Challenge packets.

Syntax

show dot1x timeout supp-timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the retransmission interval of Request/Challenge packets.

```
Hostname> enable
```

```
Hostname# show dot1x timeout supp-timeout
Supp-Timeout: 3 Seconds
```

Table 1-14 Output Fields of the show dot1x timeout supp-timeout Command

Field	Description
Supp-Timeout	Retransmission interval of Request/Challenge packets

Notifications

N/A

Platform Description

N/A

1.70 show dot1x timeout tx-period

Function

Run the **show dot1x timeout tx-period** command to display the retransmission interval of Request/Identity packets.

Syntax

show dot1x timeout tx-period

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays retransmission interval of Request/Identity packets.

```
Hostname> enable
Hostname# show dot1x timeout tx-period
Tx-Period: 30 Seconds
```

Table 1-15 Output Fields of the show dot1x timeout tx-period Command

Field	Description

Field	Description
Tx-Period	Retransmission interval of Request/Identity packets

Notifications

N/A

Platform Description

N/A

1.71 show dot1x user mac

Function

Run the **show dot1x user mac** command to display details about a user with a specified MAC address.

Syntax

show dot1x user mac *mac-address*

Parameter Description

mac-address: MAC address of a user. After this parameter is specified, details about the user are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run the **show dot1x summary** command to obtain the user MAC address from the user summary.

Examples

The following example displays details about a user with the MAC address 0023.aeaa.4286.

```
Hostname> enable
Hostname# show dot1x user mac 0023.aeaa.4286
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Inner-VLAN id 5
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
```

```
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Table 1-16 Output Fields of the show dot1x user mac Command

Field	Description
User name	Username
User id	User ID
Type	User type
Mac address	MAC address of a user
Vlan id	User VLAN ID
Inner-VLAN id	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Access from port	User port
Time online	Online duration
User ip address	IP address of a user
Max user number on this port	Maximum number of users supported by the port
Authorization session time	Authorization time of the user
Supplicant is private	Whether the user client is a Ruijie client
Start accounting	Whether accounting is started for the user
Permit proxy user	Whether the user is allowed to act as a proxy
Permit dial user	Whether the user is allowed to perform dialup
IP privilege	IP privilege level of the user
user acl-name	ACL delivered to the user

Notifications

N/A

Platform Description

N/A

1.72 show dot1x user name

Function

Run the **show dot1x user name** command to display details about a user with a specified username.

Syntax

show dot1x user name *user-name*

Parameter Description

user-name: Username. After this parameter is specified, details about a user with the username are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

After running the **show dot1x summary** command to display the user summary, you can run this command to display details about a user.

Examples

The following example displays details about a user with the username **ts-user**.

```
Hostname> enable
Hostname# show dot1x user name ts-user
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Inner-VLAN id 5Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Table 1-17 Output Fields of the show dot1x user name Command

Field	Description
User name	Username

Field	Description
User id	User ID
Type	User type
Mac address	MAC address of a user
Vlan id	User VLAN ID
Inner-VLAN id	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Access from port	User port
Time online	Online duration
User ip address	IP address of a user
Max user number on this port	Maximum number of users supported by the port
Authorization session time	Authorization time of the user
Supplicant is private	Whether the user client is a Ruijie client
Start accounting	Whether accounting is started for the user
Permit proxy user	Whether the user is allowed to act as a proxy
Permit dial user	Whether the user is allowed to perform dialup
IP privilege	IP privilege level of the user
user acl-name	ACL delivered to the user

Notifications

N/A

Platform Description

N/A

1 Web Authentication Commands

Command	Function
accounting	Configure the accounting method list used by a template.
app-name	Configure the app name used by a template.
authentication	Configure the authentication method list used by a template.
bindmode	Configure the binding mode used by a template.
clear web-auth acl	Clear all whitelist configurations for web authentication.
clear web-auth direct-arp	Clear all Address Resolution Protocol (ARP) resources.
clear web-auth direct-host	Clear all authentication-exempted users.
clear web-auth direct-site	Clear all authentication-free network resources.
clear web-auth user	Force a user offline.
domain	Enable automatic adding of domain information after usernames.
fmt	Configure the URL format of redirection packets.
http redirect direct-arp	Configure a straight-through ARP resource range.
http redirect direct-site	Configure an authentication-free network resource range.
http redirect port	Redirect HTTP requests with specified port numbers from users.
http redirect session-limit	Configure the global maximum number of HTTP sessions allowed for an unauthenticated user.
http redirect timeout	Configure the redirection connection timeout time.
ip	Configure the IPv4 address and virtual routing and forwarding (VRF) instance of the portal server.
ip portal source-interface	Configure the portal communication source port.
port	Configure the communication port of the portal server.

redirect	Configure the encapsulation format of redirection packets.
show web-auth acl	Display whitelist configurations.
show web-auth app-config	Display app configurations.
show web-auth authmng	Display web authentication data.
show web-auth control	Display controlled authentication configurations.
show web-auth direct-arp	Display the straight-through ARP resource range.
show web-auth direct-host	Display the authentication-exempted user range.
show web-auth direct-site	Display the straight-through website range.
show web-auth ip-mapping	Display the mapping between servers and users.
show web-auth parameter	Display basic parameter configurations for web authentication.
show web-auth portal-check	Display portal-check parameters.
show web-auth rdport	Display the intercepted TCP ports.
show web-auth syslog ip	Display user online and offline records.
show web-auth template	Display the portal server configurations.
show web-auth user	Display online information of all users or a specified user, including the IP address, interface, and online time.
url	Configure the authentication page address of the portal server.
web-auth acl	Configure a whitelist.
web-auth apply-mapping	Apply the template mapping method on an interface.
web-auth dhcp-check	Enable Dynamic Host Configuration Protocol (DHCP) address check for web authentication.
web-auth dhcp-check vlan	Enable DHCP address check for web authentication on an interface.
web-auth dhcp-check disable	Disable DHCP address check on a VLAN.
web-auth direct-host	Configure the authentication-exempted user range.
web-auth enable	Enable web authentication on a port.
web-auth import-ssl	Upload the certificate and key files.

web-auth linkdown-timeout	Configure the authenticated user logout delay after a port is down.
web-auth logging enable	Configure the web authentication logging function.
web-auth mapping	Configure the webauth template mapping method.
web-auth portal direct-auth	Enable the function of adding the authentication page to Favorite.
web-auth portal extension	Enable portal specification extension.
web-auth portal key	Configure the communication key between the NAS and the portal server.
web-auth portal-check	Enable portal server detection.
web-auth portal-escape	Enable the portal escape function.
web-auth portal-import attr-26	Enable transparent transmission of RADIUS attributes.
web-auth portal-valid unique-name	Enable uniqueness check of portal authentication accounts.
web-auth radius-escape	Enable RADIUS server escape for web authentication.
web-auth ssl-policy https-redirect	Apply the HTTPS certificate and key files.
web-auth template	Create an authentication template and enter the authentication template configuration mode.
web-auth update-interval	Configure the interval for updating online user information.
web-auth vlan-control	Configure VLAN-based authentication on a port.

1.1 accounting

Function

Run the **accounting** command to configure the accounting method list used by a template.

Run the **no** form of this command to remove this configuration.

The default accounting method list is used by a template by default.

Syntax

accounting *method-list*

no accounting

Parameter Description

method-list: Name of the accounting method list used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

Before you configure an accounting method list, ensure that the accounting methods in the list have been configured on the Authentication, Authorization and Accounting (AAA) module and the method list name is the same as that configured in the AAA module.

The same authentication method needs to be used for IPv4 and IPv6 packets.

Examples

The following example configures accounting method list mlist1 for template eportalv2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# accounting mlist1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa accounting network** (AAA)

1.2 app-name

Function

Run the **app-name** command to configure the app name used by a template.

Run the **no** form of this command to remove this configuration.

Syntax

app-name { **APP_AUTH** | *app-name* }

no app-name

Parameter Description

APP_AUTH: Configures the gateway authentication app.

app-name: App name used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The name of the app interworking with the web authentication module must be correctly configured.

Examples

The following example sets the app name used by a template to **appauth**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template appauth
Hostname(config.tmplt.app)# app-name appauth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth template**

1.3 authentication

Function

Run the **authentication** command to configure the authentication method list used by a template.

Run the **no** form of this command to remove this configuration.

The default authentication method list is used by a template by default.

Syntax

authentication *method-list*

no authentication

Parameter Description

method-list: Name of the authentication method list used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The authentication method list name configured by running this command must be the same as that configured in the AAA module.

The first-generation web authentication does not support the configuration of an authentication method list.

Examples

The following example configures authentication method list mlist1 for template eportalv2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# authentication mlist1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa authentication web-auth** (AAA)
- **web-auth template**

1.4 bindmode

Function

Run the **bindmode** command to configure the binding mode used by a template.

Run the **no** form of this command to remove this configuration.

The default binding mode used by a template is IP address+MAC address.

Syntax

bindmode { **ip-mac-mode** | **ip-only-mode** }

no bindmode

Parameter Description

ip-mac-mode: Specifies the IP address+MAC address binding mode. In this mode, both the IP address and media access control (MAC) address are used in the forwarding entry.

ip-only-mode: Specifies the IP address binding mode. In this mode, only the IP address is used in the forwarding entry. You are advised to use this binding mode in layer 3 (L3) networks because MAC address information in L3 networks is incorrect.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the binding mode used by template eportalv2 to IP address only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# bindmode ip-only-mode
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth template**

1.5 clear web-auth acl

Function

Run the **clear web-auth acl** command to clear all whitelist configurations for web authentication.

Syntax

clear web-auth acl white-url

Parameter Description

white-url: Clears all whitelisted URLs.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all whitelisted URLs for web authentication.

```
Hostname> enable
Hostname# clear web-auth acl white-url
```

Notifications

N/A

Platform Description

N/A

1.6 clear web-auth direct-arp

Function

Run the **clear web-auth direct-arp** command to clear all Address Resolution Protocol (ARP) resources.

Syntax

clear web-auth direct-arp

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all ARP resources.

```
Hostname> enable
Hostname# clear web-auth direct-arp
```

Notifications

N/A

Platform Description

N/A

1.7 clear web-auth direct-host

Function

Run the **clear web-auth direct-host** command to clear all authentication-exempted users.

Syntax

clear web-auth direct-host

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all authentication-exempted users.

```
Hostname> enable
Hostname# clear web-auth direct-host
```

Notifications

N/A

Platform Description

N/A

1.8 clear web-auth direct-site

Function

Run the **clear web-auth direct-site** command to clear all authentication-free network resources.

Syntax

clear web-auth direct-site

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all authentication-free network resources.

```
Hostname> enable
Hostname# clear web-auth direct-site
```

Notifications

N/A

Platform Description

N/A

1.9 clear web-auth user

Function

Run the **clear web-auth user** command to force a user offline.

Syntax

clear web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }

Parameter Description

all: Forces all users offline.

ip *ipv4-address*: Forces users with specified IPv4 addresses offline.

mac *mac-address*: Forces users with specified MAC addresses offline.

name *name*: Forces users with specified usernames offline.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example forces all users offline.

```
Hostname> enable
Hostname# clear web-auth user all
```

Notifications

N/A

Platform Description

N/A

1.10 domain

Function

Run the **domain** command to enable automatic adding of domain information after usernames.

Run the **no** form of this command to remove this configuration.

No domain information is added after usernames by default.

Syntax

domain *domain-info*

no domain

Parameter Description

domain-info: Domain information to be automatically added after usernames. The value is a string of 1 to 63 bytes.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

Not all templates support automatic adding of domain information after usernames. Template eportalv1 does not support, while template eportalv2 supports.

Examples

The following example configures automatic adding of domain information "@wifi" after usernames.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# domain @wifi
```

Notifications

N/A

Platform Description

N/A

1.11 fmt

Function

Run the **fmt** command to configure the URL format of redirection packets.

Run the **no** form of this command to remove this configuration.

The Ruijie URL format is used for redirection packets by default.

Syntax

URL format defined for the first-generation web authentication template:

fmt { **ace** | **default** }

URL format defined for the second-generation web authentication template:

fmt { **cmcc-ext1** | **cmcc-ext2** | **cmcc-ext3** | **cmcc-mtx** | **cmcc-normal** | **ct-jc** | **cucc** | **default** }

Custom URL format:

fmt custom [**encry** { **md5** | **des** | **des_ecb** | **des_ecb3** | **none** }] [**user-ip** *user-ip-string*] [**user-mac** *user-mac-string* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**user-vid** *user-vid-string*] [**user-id** *user-id-string*] [**nas-ip** *nas-ip-string*] [**nas-id** *nas-id-string*] [**nas-id2** *nas-id2-string*] [**ap-mac** *ap-mac-string* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**url** *url-string*] [**ssid** *ssid-string*] [**port** *port-string*] [**ac-serialno** *ac-serialno-string*] [**ap-serialno** *ap-serinalno-string*] [**additional** *additional-string*] [**nas-name** *nas-name-string*]

no fmt

no fmt custom [**user-ip**] [**user-mac**] [**user-vid**] [**user-id**] [**nas-ip**] [**nas-id**] [**nas-id2**] [**ap-mac**] [**url**] [**ssid**] [**port**] [**ac-serialno**] [**ap-serialno**] [**additional**] [**nas-name**]

Parameter Description

cmcc-ext1: Configures the extended URL format of China Mobile Communications Corporation (CMCC).

cmcc-ext2: Configures the URL format of Liaoning Mobile.

cmcc-ext3: Configures the URL format that Ningbo/Jiaxing Mobile specifies for access controller (AC) vendors.

cmcc-mtx: Configures the URL format that CMCC specifies for AC vendors.

cmcc-normal: Configures the standard URL format of CMCC.

ct-jc: Configures the URL format of China Telecom for collection projects.

cucc: Configures the URL format of Shandong Unicom.

default: Configures the default Ruijie URL format for redirection packets.

ace: Supports access control entry (ACE) association.

custom: Specifies the custom format.

md5: Configures MD5 encryption for parameters.

des: Configures Data Encryption Standard (DES) encryption for parameters.

des_ecb: Configures des_ecb encryption for parameters.

des_ecb3: Configures des_ecb3 encryption for parameters.

none: Configures plaintext parameter transmission.

user-ip *user-ip-string*: Specifies the IP address of a user.

user-mac *user-mac-string*: Specifies the MAC address of a user.

dot: Configures the MAC address format as xxxx.xxxx.xxxx.

line: Configures the MAC address format as xx-xx-xx-xx-xx-xx.

none: Configures the MAC address format as xxxxxxxxxxxx.

5colon: Configures the MAC address format as xx:xx:xx:xx:xx:xx.

user-vid *user-vid-string*: Specifies the virtual local area network ID (VID) of a user.

user-id *user-id-string*: Specifies the user ID.

nas-ip *nas-ip-string*: Specifies the IP address of the network access server (NAS).

nas-id *nas-id-string*: Specifies the ID of the NAS.

nas-id2 *nas-id2-string*: Specifies the ID of the other NAS. (Two **nas-id** parameters can be customized.)

ap-mac *ap-mac-string*: Specifies the MAC address of the associated access point (AP).

url *url-string*: Specifies the original access URL of a user.

ssid *ssid-srting*: Specifies the Service Set Identifier (SSID) name.

port *port-string*: Specifies the user authentication port.

ac-serialno *ac-serialno-string*: Specifies the serial number (SN) of an AC.

ap-serialno *ap-serinalno-string*: Specifies the SN of an AP.

additional *additional-string*: Specifies a fixed string. Some portal servers need to be identified by special character strings.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The URL format needs to be configured based on the interworking specifications of the portal server.

Examples

The following example sets the URL format of redirection packets to the CMCC extended format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# fmt cmcc-ext1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 http redirect direct-arp

Function

Run the **http redirect direct-arp** command to configure a straight-through ARP resource range.

Run the **no** form of this command to remove this configuration.

No straight-through ARP resource range is configured by default.

Syntax

http redirect direct-arp *ipv4-address* [*mask*]

no http redirect direct- arp *ipv4-address* [*mask*]

Parameter Description

ipv4-address: IPv4 address configured as a straight-through ARP resource.

mask: Mask of the IPv4 address configured as a straight-through ARP resource.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When ARP check is enabled, users cannot learn the ARP entries of the gateway or other devices. You can run this command to permit ARP learning for a specified address or network segment.

When ARP check is enabled, you need to configure the gateway of the PCs connecting to the L2 access device as a straight-through ARP resource.

If both straight-through websites and ARP resources are configured for the same address/network segment, the commands will be combined automatically.

If no ARP option is specified in the straight-through website configuration, the option will be added automatically after combination.

When ARP check is enabled, if the outbound interface address of the PC connecting to the L2 access device is not the gateway address, you need to configure the outbound interface address as a straight-through ARP resource. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.

If ARP check is enabled, you must configure the authentication-free network resources and gateway address as straight-through ARP resources.

Examples

The following example configures the website whose IP address is 172.16.0.1 as a straight-through ARP resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-arp 172.16.0.1
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 http redirect direct-site

Function

Run the **http redirect direct-site** command to configure an authentication-free network resource range.

Run the **no** form of this command to remove this configuration.

No authentication-free network resource range is configured by default.

Syntax

http redirect direct-site *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]
no http redirect direct-site *ipv4-address* [*mask*]

Parameter Description

ipv4-address: IPv4 address configured as an authentication-free network resource.

mask: Mask of the IPv4 address configured as an authentication-free network resource.

arp: Performs ARP binding for the authentication-free network resource range when the APR check function is enabled, that is, configures the **arp** keyword. This field is required only when IPv4 network resources are configured.

port-number&<1-8>: Authentication-free L4 port. &<1-8> indicates that the parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The number of authentication-free network resources and the number of authentication-exempted users cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

Examples

The following example configures the website whose IPv4 address is 172.16.0.1 as an authentication-free network resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-site 172.16.0.1
```

The following example configures the website whose MAC address is 0000:5e00:0101 as an authentication-free network resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-site 0000:5e00:0101
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 http redirect port

Function

Run the **http redirect port** command to redirect HTTP requests with specified port numbers from users.

Run the **no** form of this command to remove this configuration.

The NAS intercepts HTTP packets with port numbers 80 and 443 from users and redirects them to the authentication page by default.

Syntax

http redirect port *port-number*

no http redirect port *port-number*

Parameter Description

port-number: Port number in HTTP requests to be intercepted. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The NAS needs to intercept HTTP packets with specified port numbers from users and redirect these HTTP packets to the authentication page to complete authentication. The port numbers can be configured.

A maximum of 10 different destination port numbers can be configured, excluding default ports 80 and 443.

The commonly used management ports on the access or convergence device, such as ports 22, 23, and 53, and ports reserved by the system are not allowed to be configured as the redirection port.

HTTP seldom uses ports with numbers smaller than 1000 except port 80. To avoid a conflict with well-known Transmission Control Protocol (TCP) ports, do not configure a port with a small number as the redirection port.

Examples

The following example redirects HTTP requests with destination port number 8080 from users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect port 8080
```

The following example does not redirect HTTP requests with destination port number 80 from users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no http redirect port 80
```

Notifications

When HTTP requests with the destination port set to a well-known protocol port or internal reserved port, for example, port 23, are intercepted, the following notification will be displayed:

```
%Error: Can't set local reserved port(23) as redirection port.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 http redirect session-limit

Function

Run the **http redirect session-limit** command to configure the global maximum number of HTTP sessions allowed for an unauthenticated user.

Run the **no** form of this command to remove this configuration.

The global maximum number of HTTP sessions allowed for an unauthenticated user is **255** by default.

Syntax

http redirect session-limit *session-number*

no http redirect session-limit

Parameter Description

session-number: Global maximum number of HTTP sessions allowed for an unauthenticated user. The value range is from 1 to 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

TCP connection resources may be exhausted if unauthenticated users initiate excessive HTTP attacks. Therefore, it is necessary to restrict the maximum number of HTTP sessions allowed for unauthenticated users on the NAS. User authentication occupies one HTTP session, and other applications of a user may also need HTTP sessions. Therefore, you are not advised to set the maximum number of HTTP sessions to 1 for unauthenticated users.

If the authentication page fails to be displayed during web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that occupy HTTP sessions and perform web authentication again.

Examples

The following example sets the global maximum number of HTTP sessions allowed for an unauthenticated user to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect session-limit 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 http redirect timeout

Function

Run the **http redirect timeout** command to configure the redirection connection timeout time.

Run the **no** form of this command to remove this configuration.

The default redirection connection timeout time is **3** seconds.

Syntax

http redirect timeout *timeout*

no http redirect timeout

Parameter Description

timeout: Redirection connection timeout time, in seconds. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

HTTP redirection is implemented by establishing a TCP connection between the NAS and a user host and adding the redirection page URL to the 302 packet replied by the NAS. After a TCP connection is established between the NAS and a user host, the TCP connection is closed after the NAS receives an HTTP GET/HEAD packet from the user host and responds with an HTTP redirection packet.

The redirection connection timeout time prevents a TCP connection being occupied for a long time because the user host does not send a GET/HEAD packet. After the timeout time expires, the NAS will forcibly disconnect the TCP connection.

Examples

The following example sets the redirection connection timeout time to 4 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect timeout 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip

Function

Run the **ip** command to configure the IPv4 address and virtual routing and forwarding (VRF) instance of the portal server.

Run the **no** form of this command to remove this configuration.

No portal server IPv4 address or VRF instance is configured by default.

Syntax

ip [*ipv4-address* | **oob** | **vrf** *vrf-name*]

no ip [**oob** | **vrf**]

Parameter Description

ipv4-address: IPv4 address of the portal server.

oob: Uses the MGMT port for communication.

vrf *vrf-name*: Specifies the virtual private network (VPN) instance name.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IP address of the portal server for redirection in template eportalv1 to 172.16.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# ip 172.16.0.1
```

Notifications

When the portal server IP address is changed directly, the following notification will be displayed:

```
%Error: Modify portal ip is unsupportted.
```

When an invalid IP address is set, the following notification will be displayed:

```
%Error: Invalid portal ip address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip portal source-interface

Function

Run the **ip portal source-interface** command to configure the portal communication source port.

Run the **no** form of this command to remove this configuration.

No portal communication source port is configured by default.

Syntax

ip portal source-interface *interface-type interface-num*

no ip portal source-interface

Parameter Description

interface-type interface-number: Type and number of the interface used for portal communication.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the portal communication source port is configured, the NAS uses the source port to communicate with the portal server, and the used source IP address is the IP address configured on the source port.

Only one portal communication source port can be configured.

Examples

The following example configures Aggregateport 1 as the portal communication source port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip portal source-interface aggregateport 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 port

Function

Run the **port** command to configure the communication port of the portal server.

Run the **no** form of this command to remove this configuration.

The default portal server communication port is **50100** for second-generation web authentication and **80** for app-based authentication.

Syntax

port *port-number*

no port

Parameter Description

port-number: Communication port of the portal server. The value range is from 1 to 65535.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the communication port of the portal server to 10000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# port 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 redirect

Function

Run the **redirect** command to configure the encapsulation format of redirection packets.

Run the **no** form of this command to remove this configuration.

Redirection packets of the Ruijie URL format use the JaveScript (JS) encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

Syntax

redirect { **http** | **js** }

no redirect

Parameter Description

http: Uses the HTTP 302 packet for URL redirection.

js: Uses the HTTP 200 packet with JS for URL redirection.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the encapsulation format of redirection packets to http.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# redirect http
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show web-auth acl

Function

Run the **show web-auth acl** command to display whitelist configurations.

Syntax

show web-auth acl white-url

Parameter Description

white-url: Displays whitelisted URLs.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays whitelist configurations.

```
Hostname> enable
Hostname# show web-auth acl white-url
White URL List:0
-----------------------------------------------------------
```

Table 1-1 Output Fields of the show web-auth acl Command

Field	Description
White URL List	Whitelisted URLs

Notifications

N/A

Platform Description

N/A

1.22 show web-auth app-config

Function

Run the **show web-auth app-config** command to display app configurations.

Syntax

show web-auth app-config *app-name*

Parameter Description

app-name: Name of the app whose configurations are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display app configurations.

Examples

The following example displays configurations of the app test_app.

```
Hostname> enable
Hostname# show web-auth app-config test_app
-----escape----
enable: ON
escape_online: 1
```

```
escape_url:
no_kick: 1
```

Table 1-2 Output Fields of the show web-auth app-config test_app Command

Field	Description
enable	Whether the escape function is enabled
escape_online	Whether to allow users to go online automatically after escape is triggered
escape_url	URL to which a user is redirected after escape is triggered
no_kick	Whether to force online users offline when escape is triggered

Notifications

N/A

Platform Description

N/A

1.23 show web-auth authmng

Function

Run the **show web-auth authmng** command to display web authentication data.

Syntax

show web-auth authmng [**abnormal** | **statistic**]

Parameter Description

abnormal: Displays web authentication exceptions.

statistic: Displays web authentication statistics.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays web authentication statistics.

```
Hostname> enable
Hostname# show web-auth authmng statistic
```

```
Show web authentication information:
 current online number:.................................0.
 historical max online number:..........................0.
 aggregate online number:...............................0.

Web authentication redirect statistic:
 HTTP packet processing:
  number of users:.....................................0
  number of HTTP packets received:.....................0
 redirection time consumption for successful users:
  average time consumption:.............................0ms.
  aggregate time consumption:...........................0ms.
  number of less than half one second:..................0(0.000%).
  number of between half and one second:................0(0.000%).
  number of more than one second:.......................0.

Web authentication statistic:
 authentication processing:
  number of authentication requests received:...........0.
  number of reauthentication requests received:.........0.
  number of error password:.............................0.
  number of authentication failures:....................0(0.000%).
   AAA timeout:........................................0(0.000%).
   authentication status timeout:......................0(0.000%).
   fail to set SCC:....................................0(0.000%).
   accounting reject:..................................0(0.000%).
   accounting dev timeout:.............................0(0.000%).
   user unexist:.......................................0(0.000%).
   portal timeout:.....................................0(0.000%).
   DHCPrelease pkt:....................................0(0.000%).
   sta move:...........................................0(0.000%).
   clear user:.........................................0(0.000%).
   config change:......................................0(0.000%).
   other:..............................................0.
 authentication time consumption for successful users:
  average time consumption:.............................0ms.
  aggregate time consumption:...........................0ms.
  number of less than one second:.......................0(0.000%).
  number of between one and three second:...............0(0.000%).
  number of more than three second:.....................0(0.000%).
  number of less than one second(exclude server):.......0(0.000%).
  number of between one and three second(exclude server):0(0.000%).
  number of more than three second(exclude server):.....0(0.000%).

Web authentication offline information:
 number of offline count:..............................0.
```

```
  number of abnormal offline(rate):.....................0(0.000%).
   number of portal timeout:............................0(0.000%).
   number of set fail:..................................0(0.000%).
   number of link change:...............................0.
  no flow:.............................................0.
  kick off:............................................0.
  dhcp release:........................................0.
  STA delete:..........................................0.
  STA move:............................................0.
  active offline:......................................0.
  session timeout:.....................................0.
  cli clear:...........................................0.
  no control:..........................................0.
  interface default:...................................0.
  interface destroy:...................................0.
  dhcp ip check:.......................................0.
  vlan change:.........................................0.
  intfvlan change:.....................................0.
  other:...............................................0.
 aggregate online time:...............................0min
 average online time of user:.........................0min

Station-move:
 move count:..........................................0.
 move fail:...........................................0.

Other important process statistics:
Auth:
 average time consumption:............................0ms.
 aggregate time consumption:..........................0ms.
 number of less than one second:......................0(0.000%).
 number of more than one second:......................0.

AAA authentication:
 average time consumption:............................0ms.
 aggregate time consumption:..........................0ms.
 number of less than one second:......................0(0.000%).
 number of more than one second:......................0.

Radius authentication:
 average time consumption:............................0ms.
 aggregate time consumption:..........................0ms.
 number of less than one second:......................0(0.000%).
 number of more than one second:......................0.

Radius server authentication:
```

```
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

SCC:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

Accounting:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

AAA accounting:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

Radius accounting:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

Radius server accounting:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.

Portal:
 average time consumption:.............................0ms.
 aggregate time consumption:...........................0ms.
 number of less than one second:.......................0(0.000%).
 number of more than one second:.......................0.
```

Table 1-3 Output Fields of the show web-auth authmng statistic Command

Field	Description
Show web authentication information	Web authentication information

Field	Description
current online number	Number of online users
historical max online number	Historical maximum number of online users
aggregate online number	Accumulated number of online users
Web authentication redirect statistic	User redirection statistics
HTTP packet processing	HTTP packet processing
number of users	Number of redirected users
number of HTTP packets received	Number of received HTTP packets
redirection time consumption for successful users	Time required for redirection
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than half one second	Number of users whose redirection time is less than 0.5s
number of between half and one second	Number of users whose redirection time is from 0.5s to 1s
number of more than one second	Number of users whose redirection time is greater than 1s
Web authentication statistic	Web authentication statistics
authentication processing	Authentication
number of authentication requests received	Number of authentication requests
number of reauthentication requests received	Number of re-authentication requests
number of error password	Number of authentication failures due to incorrect passwords
number of authentication failures	Number of authentication failures due to other causes
AAA timeout	Number of AAA timeout times
authentication status timeout	Number of authentication timeout times
fail to set SCC	Number of SCC configuration failures
accounting reject	Number of rejected accounting times
accounting dev timeout	Number of accounting timeout times
user unexist	Number of times with non-existent users

Field	Description
portal timeout	Number of portal server timeout times
DHCPrelease pkt	Number of DHCP release times
sta move	Number of user migration times
clear user	Number of user clearing times
config change	Number of configuration changes
other	Number of authentication failures due to other reasons
authentication time consumption for successful users	Time required for successful authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of between one and three second	Number of users whose authentication time is from 1s to 3s
number of more than three second	Number of users whose authentication time is greater than 3s
number of less than one second(exclude server)	Number of users whose authentication time is less than 1s excluding the time for interaction between the NAS and portal server
number of between one and three second(exclude server)	Number of users whose authentication time is from 1s to 3s excluding time for interaction between the NAS and the portal server
number of more than three second(exclude server)	Number of users whose authentication time is greater than 3s excluding time for interaction between the NAS and the portal server
Web authentication offline information	Web authentication user offline information
number of offline count	Total number of offline times
number of abnormal offline(rate)	Number of abnormal offline times
number of portal timeout	Number of portal server timeout times
number of set fail	Number of entry configuration failures
number of link change	Number of link changes
no flow	Number of offline times due to no traffic
kick off	Number of times being kicked off by the server
dhcp release	Number of DHCP release times

Field	Description
STA delete	Number of STA deletion times
STA move	Number of STA migration times
active offline	Number of offline times requested by users
session timeout	Number of times with the online duration expired
cli clear	Number of users cleared in the command-line interface (CLI)
no control	Number of users who go offline because web control is disabled
interface default	Number of users who go offline because an interface is restored to the default configuration
interface destroy	Number of users who go offline because an interface is deleted
dhcp ip check	Number of users who go offline because the DHCP IP address is changed
vlan change	Number of users who go offline due to VLAN changes
intfvlan change	Number of users who go offline due to L3 VLAN configuration changes
other	Number of users who go offline due to other causes
aggregate online time	Accumulated online duration
average online time of user	Average online duration of users
Station-move	User migration
move count	Total number of migrated users
move fail	Migration failed
Other important process statistics	Other important data
Auth	Authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
AAA authentication	AAA Authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time

Field	Description
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
Radius authentication	RADIUS authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
Radius server authentication	RADIUS server authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
SCC	SCC
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
Accounting	Accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
AAA accounting	AAA accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
Radius accounting	RADIUS accounting

Field	Description
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
Radius server accounting	RADIUS accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s

The following example displays abnormal authentication data.

```
Hostname> enable
Hostname# show web-auth authmng abnormal
record num:0, value:3000, max-num:1000, clock:1
```

Table 1-4 Output Fields of the show web-auth authmng abnormal Command

Field	Description
Record num	Number of abnormal records
value	Conditions for identifying abnormal records, that is, the timeout time. A record with 3s or longer authentication time is an abnormal record by default.
max-num	Maximum number of allowed records
clock	Time when a record is written to the flash memory. The default value is 01:00:00 [0–23].

Notifications

N/A

Platform Description

N/A

1.24 show web-auth control

Function

Run the **show web-auth control** command to display controlled authentication configurations.

Syntax

show web-auth control

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays controlled authentication configurations.

```
Hostname> enable
Hostname# show web-auth control
 Port                  Control  Server Name         Online User Count Arp-detect
Vlan Control List
 ---------------------------- --------
 GigabitEthernet 0/1      On      eportalv2           1               On
```

Table 1-5 Output Fields of the show web-auth control Command

Field	Description
Port	Name of a controlled port
Control	Whether web authentication is enabled for a port
Server Name	Customized server name on the port. <not configured> indicates that no server name is configured.
Online User Count	Number of online users on a port
Arp-detect	Whether ARP detection for user migration is enabled
Vlan Control List	List of VLANs that can be authenticated

Notifications

N/A

Platform Description

N/A

1.25 show web-auth direct-arp

Function

Run the **show web-auth direct-arp** command to display the straight-through ARP resource range.

Syntax

show web-auth direct-arp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the straight-through ARP resource range.

```
Hostname> enable
Hostname# show web-auth direct-arp
Direct arps:
  Address        Mask
  ----- ----
  1.1.1.1        255.255.255.255
  2.2.2.2        255.255.255.255
```

Table 1-6 Output Fields of the show web-auth direct-arp Command

Field	Description
Address	IP address
Mask	Mask of an IP address

Notifications

N/A

Platform Description

N/A

1.26 show web-auth direct-host

Function

Run the **show web-auth direct-host** command to display the authentication-exempted user range.

Syntax

show web-auth direct-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all authentication-exempted users.

```
Hostname> enable
Hostname# show web direct-host
Direct hosts: 1
  Address        Mask          Port Binding   ARP Binding   Access Port List
  ----- ----- ---------- -----
  1.1.1.1        255.255.255.255 N/A          Off          1080
  Index     MAC-Address
  --------
```

Table 1-7 Output Fields of the show web direct-host Command

Field	Description
Address	IP address of an authentication-exempted user
Mask	Mask of the IP address of an authentication-exempted user
Port Binding	Device port bound to the IP address of an authentication-exempted user
ARP Bining	Whether ARP binding is performed
Access Port List	Bound L4 port list

Notifications

N/A

Platform Description

N/A

1.27 show web-auth direct-site

Function

Run the **show web-auth direct-site** command to display the straight-through website range.

Syntax

show web-auth direct-site

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all straight-through websites.

```
Hostname> enable
Hostname# show web-auth direct-site
Direct sites: 2
  Address                          Mask          ARP Binding   Ports
  ------------- ----- --------
  1.1.1.1                          255.255.255.255 Off          N/A
  2.2.2.2                          255.255.255.255 Off          1080 2080
```

Table 1-8 Output Fields of the show web-auth direct-site Command

Field	Description
Addres	IP address
Mask	Mask of an IP address
ARP Binding	Whether ARP binding is performed
Ports	L4 straight-through port

Notifications

N/A

Platform Description

N/A

1.28 show web-auth ip-mapping

Function

Run the **show web-auth ip-mapping** command to display the mapping between servers and users.

Syntax

show web-auth ip-mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mapping between servers and users.

```
Hostname> enable
Hostname# show web-auth ip-mapping
-------------------
  Name:      iportal
  Ip:        0.0.0.0
  Url:
  Ip-Mapping:
-------------------
  Name:      eportalv1
  Ip:        172.18.105.9
  Url:       http://172.18.105.9:8080/eportal/index.jsp
  Ip-Mapping:
            1.1.1.0-255.255.255.0         Global
```

Table 1-9 Output Fields of the show web-auth ip-mapping Command

Field	Description
Name	Mapping method name
Ip	Mapped IP address

Field	Description
Url	Mapped URL
Ip-Mapping	Mapped network segment

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show web-auth parameter

Function

Run the **show web-auth parameter** command to display basic parameter configurations for web authentication.

Syntax

show web-auth parameter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays HTTP redirection configurations.

```
Hostname> enable
Hostname# show web-auth parameter
  session-limit: 10
  timeout:       5
```

Table 1-10 Output Fields of the show web-auth parameter Command

Field	Description
session-limit	Maximum number of HTTP sessions allowed for an unauthenticated user
timeout	Redirection connection timeout time

Notifications

N/A

Platform Description

N/A

1.30 show web-auth portal-check

Function

Run the **show web-auth portal-check** command to display portal-check parameters.

Syntax

show web-auth portal-check

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays portal-check parameters.

```
Hostname> enable
Hostname# show web portal-check
Check:        Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
Escape:       Enable
Nokick:       Disable
```

Table 1-11 Output Fields of the show web portal-check Command

Field	Description
Check	Whether the portal-check function is enabled
Interval	Detection interval
Timeout	Detection timeout time
Retransmit	Number of retransmission times for each detection
Escape	Whether portal escape is enabled
Nokick	Whether to force online users offline if the portal server is unavailable after the escape function is enabled

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 show web-auth rdport

Function

Run the **show web-auth rdport** command to display the intercepted TCP ports.

Syntax

show web-auth rdport

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the intercepted TCP ports.

```
Hostname> enable
Hostname# show web-auth rdport
Rd-Port:
80 443
```

Table 1-12 Output Fields of the show web-auth rdport Command

Field	Description
Rd-Port	Redirection port

Notifications

N/A

Platform Description

N/A

1.32 show web-auth syslog ip

Function

Run the **show web-auth syslog ip** command to display user online and offline records.

Syntax

show web-auth syslog ip *ipv4-address*

Parameter Description

ipv4-address: IPv4 address of a user whose online and offline records are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays online and offline records of a user whose IP address is 192.168.197.35.

```
Hostname> enable
Hostname# show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35  Core-index 0 Current index 2
Index:          0
```

```
 Time:           2015-10-16 20:37:34
 Behavior:        ONLINE
 Mac:            00d0.f822.33e7
 Vid:            101
 Port:           Gi3/1
 Timeused:        0d 00:00:00
 Flow_up:         0
 Flow_down:       0
Index:          1
 Time:           2015-10-16 20:42:08
 Behavior:        OFFLINE
 Mac:            00d0.f822.33e7
 Vid:            101
 Port:           Gi3/1
 Timeused:        0d 00:04:27
 Flow_up:         2107872
 Flow_down:       2108224
```

Table 1-13 Output Fields of the show web-auth syslog ip Command

Field	Description
Index	Record No.
Time	Record occurrence time
Behavior	Online or offline action
MAC	MAC address of a user
Vid	VID of a user
Port	Port on the NAS used by user hosts to connect to the NAS
Timeused	Online time
Flow_up	Uplink traffic of a user
Flow_down	Downlink traffic of a user

Notifications

N/A

Platform Description

N/A

1.33 show web-auth template

Function

Run the **show web-auth template** command to display the portal server configurations.

Syntax

show web-auth template

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the portal server configurations.

Examples

The following example displays portal server configurations.

```
Hostname> enable
Hostname# show web-auth template
Webauth Template Settings:
-------------------
  Name:     eportalv1
  Url:      http://17.17.1.21:8080/eportal/index.jsp
  Ip:       17.17.1.21
  BindMode:  ip-mac-mode
  Type:     v1
-------------------
  Name:     eportalv2
  Url:      http://17.17.1.21:8080/eportal/index.jsp
  Ip:       17.17.1.21
  BindMode:  ip-only-mode
  Type:     v2
  Port:     50100
  Acctmlist:
  Authmlist:
```

Table 1-14 Output Fields of the show web-auth template Command

Field	Description
Name	Template name

Field	Description
Url	Homepage address of the portal server
Ip	IP address of the server
Type	Server type (v1 for first-generation web authentication, and v2 for second-generation web authentication)
Port	Communication port for protocol packets of the portal server (This parameter is valid only for the portal server of second-generation web authentication.)
Acctmlist	Accounting method list name (This parameter is valid only for second-generation web authentication.)
Authmlist	Authentication method list name (This parameter is valid only for second-generation web authentication.)

Notifications

N/A

Platform Description

N/A

1.34 show web-auth user

Function

Run the **show web-auth user** command to display online information of all users or a specified user, including the IP address, interface, and online time.

Syntax

show web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }

Parameter Description

all: Displays online information of all users.

ip *ipv4-address*: Specifies the IPv4 address of a user whose online information is displayed.

mac *mac-address*: Specifies the MAC address of a user whose online information is displayed.

name *name*: Specifies the username of a user whose online information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays online information of all users.

```
Hostname> enable
Hostname# show web user all
Current user num: 1, Online 1
Address                          Online  Time Limit     Time Used      Status  Name
-------------- --------------- -----
172.30.33.227                     On     240d 00:00:00  0d 00:01:19    Active
linlt
```

The following example displays online information of a user whose IP address is 192.168.0.11.

```
Hostname> enable
Hostname# show web-auth user ip 192.168.0.11
Address      :   192.168.0.11
 Mac          :   00d0.f800.2233
 Port         :   Gi0/2
 Online       :   On
 Time Limit   :   0d 01:00:00
 Time Used    :   0d 00:15:10
 Time Start   :   2009-02-22 20:05:10
 Status       :   Active
```

Table 1-15 Output Fields of the show web-auth user Command

Field	Description
Address	IP address of a user
Mac	MAC address of a user
Port	Port on the user host used to connect to the NAS
Online	Whether a user is online
Time Limit	Limit of the available online time of a user (The value **0** indicates no limit.)
Time Used	User online duration
Time Start	Time when a user passes authentication and starts to get online
Status	User status, including: ● **Active**: A user gets online. ● **Create**: A user is created, and settings are not completed. ● **Destroy**: A user is deleted, and settings are not cleared.
Name	Username (This field is null for users authenticated using the first-generation web authentication solution.)

Notifications

N/A

Platform Description

N/A

1.35 url

Function

Run the **url** command to configure the authentication page address of the portal server.

Run the **no** form of this command to remove this configuration.

No authentication page address of the portal server is configured by default.

Syntax

url *url-string*

no url

Parameter Description

url-string: Authentication page address of the portal server, which must be started with "http://" or "https://". The value is a string of up to 255 characters.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the authentication page address of the portal server in template eportalv1 to http://www.web-auth.net/login.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# url http://www.web-auth.net/login
```

Notifications

When an invalid URL format is used, the following notification will be displayed:

```
%Error: Invalid homepage URL.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 web-auth acl

Function

Run the **web-auth acl** command to configure a whitelist.

Run the **no** form of this command to remove this configuration.

No whitelist is configured by default.

Syntax

web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*
no web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*

Parameter Description

oob: Uses the MGMT port.

vrf *vrf-name*: Specifies the VPN instance name.

white-url *white-url-name*: Specifies whitelisted URLs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A whitelist allows users to access some network resources before authentication.

A whitelist can contain a maximum of 1000 addresses.

When whitelisted addresses are configured in domain name format, you need to configure the domain name server (DNS) function for the NAS to enable the NAS to correctly parse domain names.

Some domain names correspond to multiple IP addresses. A domain name can map to eight IP addresses at most.

Examples

The following example adds www.hostname.com to the whitelist.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth acl white-url www.hostname.com
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 web-auth apply-mapping

Function

Run the **web-auth apply-mapping** command to apply the template mapping method on an interface.

Run the **no** form of this command to remove this configuration.

No template mapping method is applied on an interface by default.

Syntax

web-auth apply-mapping *mapping-method*

no web-auth apply-mapping

Parameter Description

mapping-method: Template mapping method.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By setting the VLAN or IP address range, you can select users for whom a template mapping method needs to be configured.

Examples

The following example applies template mapping method "test" on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#web-auth apply-mapping test
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth mapping**

1.38 web-auth dhcp-check

Function

Run the **web-auth dhcp-check** command to enable Dynamic Host Configuration Protocol (DHCP) address check for web authentication.

Run the **no** form of this command to disable this feature.

DHCP address check is disabled for web authentication by default.

Syntax

web-auth dhcp-check

no web-auth dhcp-check

Parameter Description

N/A

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

To use this function, you must configure DHCP Snooping.

Only second-generation web authentication is supported for users with IPv4 addresses.

This function applies only to network environments with IP addresses assigned through DHCP. If users with statically configured IP addresses exist, network access of these users will be limited.

If only a few users need to use static IP addresses, configure these IP addresses as straight-through addresses. In this case, these users are exempted from authentication.

To apply this function to an interface, disable global DHCP address check first.

Examples

The following example enables DHCP address check for web authentication globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth dhcp-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 web-auth dhcp-check vlan

Function

Run the **web-auth dhcp-check vlan** command to enable DHCP address check for web authentication on an interface.

Run the **no** form of this command to disable this feature.

DHCP address check for web authentication is disabled on an interface by default.

Syntax

web-auth dhcp-check vlan *vlan-list*

no web-auth dhcp-check vlan *vlan-list*

Parameter Description

vlan *vlan-list*: Specifies the VLAN range on an interface for which DHCP address check needs to be enabled. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After VLAN-based authentication is configured on a port, only the user hosts in the configured VLAN can initiate web authentication.

Examples

The following example enables DHCP address check for web authentication on GigabitEthernet 0/1 and sets the detected VLAN range to 1 and 3-5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# web-auth dhcp-check vlan 1,3-5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 web-auth dhcp-check disable

Function

Run the **web-auth dhcp-check disable** command to disable DHCP address check on a VLAN.

Run the **no** form of this command to remove this configuration.

DHCP address check is enabled on a VLAN by default.

Syntax

web-auth dhcp-check vlan disable

no web-auth dhcp-check vlan disable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables DHCP address check on a VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth dhcp-check vlan disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 web-auth direct-host

Function

Run the **web-auth direct-host** command to configure the authentication-exempted user range.

Run the **no** form of this command to remove this configuration.

No IP/MAC address range of authentication-exempted users is configured by default. All users can access network resources only after they pass web authentication.

Syntax

web-auth direct-host *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]
web-auth direct-host *mac-address*
no web-auth direct-host { *ipv4-address* [*mask*] }
no web-auth direct-host *mac-address*

Parameter Description

ipv4-address: IPv4 address of an authentication-exempted user.

mask: Mask of the IP address of an authentication-exempted user.

arp: Performs ARP binding for network resources of authentication-exempted users when the APR check function is enabled, that is, configures the **arp** keyword. This field is required only when IPv4 network resources are configured.

port-number&<1-8>: L4 port of an authentication-exempted user. &<1-8> indicates that the parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.

mac-address: MAC address of a user exempted from authentication.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The number of authentication-exempted users and the number of authentication-free network resources cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

Examples

The following example configures the user whose IPv4 address is 172.16.0.1 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host 172.16.0.1
```

The following example configures the user whose IPv6 address is FF02::/64 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host FF02::/64
```

The following example configures the user whose MAC address is 0000:5e00:0101 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host 0000:5e00:0101
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 web-auth enable

Function

Run the **web-auth enable** command to enable web authentication on a port.

Run the **no** form of this command to disable this feature.

The web authentication function is disabled on a port by default.

Syntax

web-auth enable [*template-name* | **appauth** | **eportalv1** | **eportalv2**]

no web-auth enable

Parameter Description

template-name: Custom template whose web authentication is enabled.

eportalv1: Enables first-generation web authentication.

eportalv2: Enables second-generation web authentication.

appauth: Enables app-based authentication.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After web authentication is enabled, the first-generation web authentication template is used by default if no parameter is specified.

To apply web authentication successfully, you must configure the authentication page address.

Examples

The following example enables web authentication on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 web-auth import-ssl

Function

Run the **web-auth import-ssl** command to upload the certificate and key files.

Syntax

web-auth import-ssl { **cert ftp:***path* | **cert tftp:***path* | **cert oob_ftp:***path* | **cert oob_tftp:***path* } { **key ftp:***path* | **key tftp:***path* | **key oob_ftp:***path* | **key oob_tftp:***path* } [**vrf** *vrf-name*]

Parameter Description

cert ftp:*path*: Configures the File Transfer Protocol (FTP) path for uploading certificate files.

cert tftp:*path*: Configures the Trivial FTP (TFTP) path for uploading certificate files.

cert oob_ftp:*path*: Configures the FTP path for uploading certificate files through the MGMT port.

cert oob_tftp:*path*: Configures the TFTP path for uploading certificate files through the MGMT port.

key ftp:*path*: Configures the FTP path for uploading key files.

Key tftp:*path*: Configures the TFTP path for uploading key files.

key oob_ftp:*path*: Configures the FTP path for uploading key files through the MGMT port.

key oob_tftp:*path*: Configures the TFTP path for uploading key files through the MGMT port.

vrf *vrf-name*: Configures the VRF instance used for uploading files.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

HTTPS is an encrypted data transmission protocol and relies on a certificate to ensure transmission security. Before enabling the HTTPS server function, you need to import an available certificate.

To configure HTTPS certificate import, first upload available HTTPS certificate and key files to the NAS and then apply the HTTPS certificate and key files.

Examples

The following example uploads the certificate and key files.

```
Hostname> enable
Hostname# configure terminal
Hostname# web-auth import-ssl cert tftp://182.168.1.1/cert.pem key
tftp://182.168.1.1/key.pem
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth ssl-policy https-redirect**

1.44 web-auth linkdown-timeout

Function

Run the **web-auth linkdown-timeout** command to configure the authenticated user logout delay after a port is down.

Run the **no** form of this command to remove this configuration.

The default authenticated user logout delay after a port is down is **60** seconds.

Syntax

web-auth linkdown-timeout *linkdown-timeout*

no web-auth linkdown-timeout

Parameter Description

linkdown-timeout: Authenticated user logout delay after a port is down, in seconds. The value range is from 1 to 604800.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the authenticated user logout delay is configured on a port, the user hosts connected to the port go offline after the delay when the port is down.

You are advised to configure this function to prevent repeated user authentication in scenarios when a port goes down and then up quickly.

Examples

The following example sets the authenticated user logout delay after a port is down to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth linkdown-timeout 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 web-auth logging enable

Function

Run the **web-auth logging enable** command to configure the web authentication logging function.

Run the **no** form of this command to disable this feature.

The web authentication logging function is disabled by default.

Syntax

web-auth logging enable *log-rate*

no web-auth logging enable

Parameter Description

log-rate: Number of logs printed every second. The value range is from 0 to 100. The value **0** indicates that the number of logs is not limited.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The logging function of the web authentication module can send log messages to the administrator to display the information and relevant events of users who get online/offline and allow users to configure a log printing rate limit.

This command applies only to logs printed in normal cases and is invalid to abnormal or critical logs.

Examples

The following example enables web authentication logging and configures no rate limit for log printing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth logging enable 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 web-auth mapping

Function

Run the **web-auth mapping** command to configure the webauth template mapping method.

Run the **no** form of this command to remove this configuration.

No webauth template mapping method is configured by default.

Syntax

web-auth mapping *mapping-method* { **vlan** *vlan-list* | **ip-mapping** *ipv4-address mask* } [**template** *tmpltate-name*]

no web-auth mapping *mapping-method* { **vlan** [*vlan-list*] | **ip-mapping** *ipv4-address mask* }

Parameter Description

mapping-method: Template mapping method.

vlan *vlan-list*: Specifies the VLAN list. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

ipv4-address mask: IPv4 network segment and mask that uses a template.

template *tmpltate-name*: Specifies the template name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The template mapping method is configured when multiple authentication scenarios exist on one port.

When web authentication is enabled on a port, and the method of template A is used, but some users do not apply to template A and want to use template B for authentication, you can configure a template mapping method for these users to enable these users to use the authentication method of template B.

By setting the VLAN or IP address range, you can select users for whom a template mapping method needs to be configured.

Examples

The following example configures template mapping method test1 for mapping between templates eportalv2 and VLANs 2-5 and VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth mapping test1 vlan 2-5,10 template eportalv2
```

The following example enables users in the network segment of 10.10.10.1 that uses template mapping method test1 to use template stu_1 for redirection.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# web-auth mapping map_test ip-mapping 10.10.10.1 255.255.255.0
template stu_1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show web-auth ip-mapping**

1.47 web-auth portal direct-auth

Function

Run the **web-auth portal direct-auth** command to enable the function of adding the authentication page to Favorite.

Run the **no** form of this command to disable this feature.

Adding the authentication page to favorite is disabled by default.

Syntax

web-auth portal direct-auth

no web-auth portal direct-auth

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The function of adding the authentication page to Favorite needs to query access interfaces of users by IP address and needs to be used together with ARP query or DHCP snooping.

Examples

The following example enables the function of adding the authentication page to Favorite.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal direct-auth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip dhcp snooping** (Security/DHCP Snooping)
- **Arp-check-check** (Security/ARP Check)

1.48 web-auth portal extension

Function

Run the **web-auth portal extension** command to enable portal specification extension.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Portal specification extension is enabled by default.

Syntax

web-auth portal extension

no web-auth portal extension

default web-auth portal extension

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Portal specification extension is enabled to support Ruijie portal servers and portal servers that comply with the CMCC WLAN Service Portal Specification.

Examples

The following example disables portal specification extension.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no web-auth portal extension
```

```
Hostname(config)# http redirect url-fmt ext1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 web-auth portal key

Function

Run the **web-auth portal key** command to configure the communication key between the NAS and the portal server.

Run the **no** form of this command to remove this configuration.

No communication key between the NAS and the portal server is configured by default.

Syntax

web-auth portal key *key*

no web-auth portal key

Parameter Description

key: Communication key between the NAS and portal server. The value is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To apply web authentication successfully, you must configure the communication key between the NAS and the portal server.

The communication key can be configured in global configuration mode only. Specifying a key for each server is not supported.

Examples

The following example sets the communication key between the NAS and the portal server to web-auth.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# web-auth portal key web-auth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 web-auth portal-check

Function

Run the **web-auth portal-check** command to enable portal server detection.

Run the **no** form of this command to remove this configuration.

The portal server detection function is disabled by default.

Syntax

web-auth portal-check [**interval** *interval*] [**timeout** *timeout*] [**retransmit** *retransmit-times*]

no web-auth porta-check

Parameter Description

interval *interval*: Specifies the detection interval, in seconds. The value range is from 1 to 1000. The default value is **10**.

timeout *timeout*: Specifies the packet timeout time, in seconds. The value range is from 1 to 1000. The default value is **5**.

retransmit *retransmit-times*: Configures the number of retransmission times upon timeout. The value range is from 1 to 100. The default value is **3**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In most networks, only one server is deployed and this function does not need to be configured.

If multiple portal servers exist, it is recommended that the detection interval and packet timeout time not be set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

Examples

The following example enables portal server detection and sets the detection interval to 20 seconds, the packet timeout time to 2 seconds, and the number of retransmission times upon timeout to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 web-auth portal-escape

Function

Run the **web-auth portal-escape** command to enable the portal escape function.

Run the **no** form of this command to disable this feature.

Portal escape is disabled by default.

Syntax

web-auth portal-escape [**nokick**]

no web-auth portal-escape

Parameter Description

nokick: Configures not to force online users offline if the portal server is unavailable after the escape function is enabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to configure this command if some key services in the network need to be maintained when the portal server is faulty. The portal server detection function also needs to be configured. When all of the configured portal servers are unavailable, new users can access the Internet without authentication.

Examples

The following example enables the portal escape function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-escape
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth portal-check**

1.52 web-auth portal-import attr-26

Function

Run the **web-auth portal-import attr-26** command to enable transparent transmission of RADIUS attributes.

Run the **no** form of this command to remove this configuration.

Transparent transmission of RADIUS attributes is disabled by default.

Syntax

web-auth portal-import attr-26

no web-auth portal-import attr-26

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command applies only to the Serverless Application Model (SAM) servers and Ruijie portal servers. If the NAS interworks with a portal server provided by other vendors, enabling this function may cause the portal server to fail to respond to packets.

Examples

The following example enables transparent transmission of RADIUS attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#web-auth portal-import attr-26
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 web-auth portal-valid unique-name

Function

Run the **web-auth portal-valid unique-name** command to enable uniqueness check of portal authentication accounts.

Run the **no** form of this command to disable this feature.

Uniqueness check of portal authentication accounts is disabled by default.

Syntax

web-auth portal-valid unique-name

no web-auth portal-vallid unique-name

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After uniqueness check of portal authentication accounts is enabled, the NAS returns an ACK_AUTH message carrying Errcode 2 to the portal server if account information of a new authenticated user is being used by an online user. Upon receiving such a reply message, some portal servers will send a "Terminal Preemption" prompt to user hosts. Generally, this function is enabled when the portal server needs to push the "Terminal Preemption" prompt to users.

Examples

The following example enables uniqueness check of portal authentication accounts.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-valid unique-name
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 web-auth radius-escape

Function

Run the **web-auth radius-escape** command to enable RADIUS server escape for web authentication.

Run the **no** form of this command to disable this feature.

RADIUS server escape for web authentication is disabled by default.

Syntax

web-auth radius-escape

no web-auth radius-escape

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the RADIUS server escape function is configured, users can still perform authentication to access the Internet when the RADIUS server fails.

Examples

The following example enables RADIUS server escape for web authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth radius-escape
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 web-auth ssl-policy https-redirect

Function

Run the **web-auth ssl-policy https-redirect** command to apply the HTTPS certificate and key files.

Run the **no** form of this command to remove this configuration.

No HTTPS certificate or key file is applied by default.

Syntax

web-auth ssl-policy https-redirect

no web-auth ssl-policy https-redurect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

HTTPS is an encrypted data transmission protocol and relies on a certificate to ensure transmission security. Before enabling the HTTPS server function, you need to import an available certificate.

To configure HTTPS certificate import, first upload available HTTPS certificate and key files to the NAS and then apply the HTTPS certificate and key files.

Examples

The following example applies the HTTPS certificate and key files.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth ssl-policy https-redirect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth import-ssl**

1.56 web-auth template

Function

Run the **web-auth template** command to create an authentication template and enter the authentication template configuration mode.

Run the **no** form of this command to remove this configuration.

No authentication template is configured by default.

Syntax

web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* **app** | *template-name* **v1** | *template-name* **v2** }

no web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* }

Parameter Description

appauth: Configures the default app-based authentication template.

eportalv1: Configures the default first-generation authentication template.

eportalv2: Configures the default second-generation authentication template.

template-name **app**: Custom app-based authentication template.

template-name **v1**: Custom first-generation authentication template.

template-name **v2**: Custom second-generation authentication template.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the default first-generation authentication template.

```
Hostname> enable
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)#
```

Notifications

When the template type is changed, the following notification will be displayed:

```
%Notice: Template has been created, it is a v2 template.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 web-auth update-interval

Function

Run the **web-auth update-interval** command to configure the interval for updating online user information.

Run the **no** form of this command to remove this configuration.

The default interval for updating online user information is **180** seconds.

Syntax

web-auth update-interval *update-interval*

no web-auth update-interval

Parameter Description

update-interval: Interval for updating online user information, in seconds. The value range is from 30 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The NAS needs to update maintained online user information, for example, the online time periodically. The interval for updating online user information can be manually configured based on different monitoring requirements for online user information in different scenarios.

The interval for updating online user information must be a multiple of 60. If the configured value is not a multiple of 60, the actual effective value is rounded up to the multiple of 60.

Examples

The following example sets the interval for updating online user information to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth update-interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 web-auth vlan-control

Function

Run the **web-auth vlan-control** command to configure VLAN-based authentication on a port.

Run the **no** form of this command to remove this configuration.

VLAN-based authentication is not configured on a port by default. Port-based authentication is used by default.

Syntax

web-auth vlan-control *vlan-list*

no web-auth vlan-control

Parameter Description

vlan-list: List of VLANs for which authentication is allowed. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After VLAN-based authentication is configured on a port, only the user hosts in the configured VLAN can initiate web authentication.

Examples

The following example allows authentication for VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth vlan-control 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 SCC Commands

Command	Function
clear access-control packet statistics	Clear the statistics about packets filtered due to access control.
direct-vlan	Configure authentication-exempted VLANs.
nac-author-user maximum	Configure the IPv4 user capacity on a port.
show access-control packet statistics	Display the statistics about packets filtered due to access control.
show direct-vlan	Display authentication-exempted VLAN configurations.
show nac-author-user	Display the IPv4 user capacity limit and the current number of IPv4 users.
station-move permit	Enable authenticated user migration.

1.1 clear access-control packet statistics

Function

Run the **clear access-control packet statistics** command to clear the statistics about packets filtered due to access control.

Syntax

clear access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose statistics about packets filtered due to access control are cleared.

vlan *vlan-id*: Specifies the virtual local area network (VLAN) whose statistics about packets filtered due to access control are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics about packets filtered due to access control on all interfaces.

```
Hostname> enable
Hostname# clear access-control packet statistics
```

The following example clears statistics about packets filtered due to access control on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear access-control packet statistics interface GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

1.2 direct-vlan

Function

Run the **direct-vlan** command to configure authentication-exempted VLANs.

Run the **no** form of this command to remove this configuration.

No authentication-exempted VLAN is configured by default.

Syntax

direct-vlan *vlan-list*

no direct-vlan [*vlan-list*]

Parameter Description

vlan-list: List of authentication-exempted VLANs. Use commas (,) to separate different VLANs. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To enable users in a VLAN to access the Internet without 802.1x or web authentication, you can configure the VLAN as an authentication-exempted VLAN.

Examples

The following example configures VLAN 2 as an authentication-exempted VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# direct-vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 nac-author-user maximum

Function

Run the **nac-author-user maximum** command to configure the IPv4 user capacity on a port.

Run the **no** form of this command to remove this configuration.

The IPv4 user capacity on a port is not limited by default.

Syntax

nac-author-user maximum *max-user-number*

no nac-author-user maximum

Parameter Description

max-user-number: Maximum IPv4 user capacity. The value range is from 1 to 1024.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

IPv4 users include those generated through 802.1x authentication, web authentication, and other binding functions. IPv4 users on a port may be generated over the port or globally. For example, when a global IPv4 user is bound to a port by running the corresponding command, the user is also calculated as a user on the port.

Examples

The following example sets the IPv4 user capacity on GigabitEthernet 0/1 to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nac-author-user maximum 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show access-control packet statistics

Function

Run the **show access-control packet statistics** command to display the statistics about packets filtered due to access control.

Syntax

show access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose statistics about packets filtered due to access control are displayed.

vlan *vlan-id*: Specifies the VLAN whose statistics about packets filtered due to access control are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display statistics about packets filtered due to access control.

Examples

The following example displays statistics about packets filtered due to access control on all interfaces.

```
Hostname> enable
Hostname# show access-control packet statistics
Interface     Discard           Passed
----   -------   ------
Gi0/1         575              NA
Gi0/2         575              NA
Gi0/3         575              NA
Vl2000        575              NA
```

The following example displays statistics about packets filtered due to access control on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show access-control packet statistics interface GigabitEthernet 0/1
Interface : GigabitEthernet 0/1
  Discard            : 14
  Passed             : NA
```

Table 1-1 Output Fields of the show access-control packet statistics Command

Field	Description
Interface	Interface name
Discard	Number of discarded packets
Passed	Number of released packets

Notifications

N/A

Platform Description

N/A

1.5 show direct-vlan

Function

Run the **show direct-vlan** command to display authentication-exempted VLAN configurations.

Syntax

show direct-vlan

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays authentication-exempted VLAN configurations.

```
Hostname> enable
Hostname# show direct-vlan
direct-vlan 5,7,100
```

Table 1-2 Output Fields of the show direct-vlan Command

Field	Description
direct-vlan	Authentication-exempted VLAN range

Notifications

N/A

Platform Description

N/A

1.6 show nac-author-user

Function

Run the **show nac-author-user** command to display the IPv4 user capacity limit and the current number of IPv4 users.

Syntax

show nac-author-user [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose IPv4 user capacity limit and the current number of IPv4 users are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the IPv4 user capacity limit and the current number of IPv4 users on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show nac-author-user interface GigabitEthernet 0/1
 Port     Cur_num  Max_num
 ----  ---  --
 Gi0/1    0        100
```

Table 1-3 Output Fields of the show nac-author-user Command

Field	Description
Port	Device port to be queried
Cur_num	Current number of IPv4 users
Max_num	IPv4 user capacity

Notifications

N/A

Platform Description

N/A

1.7 station-move permit

Function

Run the **station-move permit** command to enable authenticated user migration.

Run the **no** form of this command to disable this feature.

Authenticated user migration is disabled by default.

Syntax

station-move permit

no station-move permit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The authenticated user migration function allows an online authenticated user to switch to another physical location to perform authentication and go online again without getting offline.

The authenticated user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.

When both 802.1x authentication and port security are enabled on a port, and port security and 802.1x authentication users get online simultaneously, 802.1x authenticated users will fail to be migrated to another port to get online because the same MAC address cannot go online through different ports.

The user online detection function can kick users offline. When the authentication user migration function is not configured and a user does not proactively get offline, the user may be kicked offline by the online detection function and can implement authentication and get online in another physical location.

When an online authenticated user moves to a new physical location, the user needs to perform 802.1x or web authentication again.

Examples

The following example enables authenticated user migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# station-move permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Platform Description

N/A

Related Commands

N/A

1 Password Policy Commands

Command	Function
password policy life-cycle	Configure a password lifecycle.
password policy min-size	Configure the minimum password length.
password policy no-repeat-times	Prevent repeated use of passwords that are configured in the latest specified number of times.
password policy strong	Enable strong password detection.
password policy forced-password-modify	Enable forcible weak password change.
password policy printable-character-check	Enable the special character detection function.
service password-encryption	Enable encrypted password storage.
show password policy	Display configured password security policies.

1.1 password policy life-cycle

Function

Run the **password policy life-cycle** command to configure a password lifecycle.

Run the **no** form of this command to remove this configuration.

No password lifecycle is configured by default.

Syntax

password policy life-cycle *life-cycle*

no password policy life-cycle

Parameter Description

life-cycle: Password lifecycle, in days. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The password lifecycle defines the validity time of a password. If a user enters a password that has already expired during login, the system gives a prompt, indicating that the password has expired, and asks the user to reset the password.

The password lifecycle is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

The password lifecycle is affected when the system time is modified.

Examples

The following example sets the password lifecycle to 90 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy life-cycle 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **Username** (Basic Configuration/Basic Management)

1.2 password policy min-size

Function

Run the **password policy min-size** command to configure the minimum password length.

Run the **no** form of this command to remove this configuration.

The minimum password length is **8** by default.

Syntax

password policy min-size *min-size*

no password policy min-size

Parameter Description

min-size: Minimum password length. The value range is from 1 to 31.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The minimum password length is used to limit the length of user passwords. If the password entered by a user is shorter than the minimum password length, the system displays an error prompt, asking the user to specify another password of an appropriate length.

Examples

The following example sets the minimum password length to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy min-size 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 password policy no-repeat-times

Function

Run the **password policy no-repeat-times** command to prevent repeated use of passwords that are configured in the latest specified number of times.

Run the **no** form of this command to remove this configuration.

Repeated password use is allowed by default.

Syntax

password policy no-repeat-times *no-repeat-times*

no password policy no-repeat-times

Parameter Description

No-repeat-times: Number of times in which configured passwords cannot be repeatedly used. The value range is from 1 to 31.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The repeated password use prevention function prevents users from using historically configured passwords as new passwords. The system records passwords used by a user to a historical password list. If a newly configured password is within the list, the system gives a prompt and asks the user to specify another password. The maximum number of records in the password list can be manually configured. When the number of records in the password list reaches the limit, a new password record will overwrite the earliest password record.

The repeated password use prevention function is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

Examples

The following example enables repeated password use prevention function to disallow the use of historical passwords configured in the latest five times.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy no-repeat-times 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **username** (Basic Configuration/Basic Management)

1.4 password policy strong

Function

Run the **password policy strong** command to enable strong password detection.

Run the **no** form of this command to disable this feature.

The strong password detection function is enabled by default.

Syntax

password policy strong

no password policy strong

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Strong password detection is used to detect the complexity of a password and prevent password crackdown due to low complexity. The strong password detection function will send an alarm in the following scenarios:

- The password is the same as the corresponding account.
- The password contains only digits.
- The password contains only uppercase letters.
- The password contains only lowercase letters.

Examples

The following example enables the strong password detection function.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# password policy strong
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 password policy forced-password-modify

Function

Run the **password policy forced-password-modify** command to enable forcible weak password change.

Run the **no** form of this command to disable this feature.

Forcible weak password change is disabled by default.

Syntax

password policy forced-password-modify

no password policy forced-password-modify

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The forcible weak password change function is used together with another password policy (such as the minimum password length or strong password detection).

After the forcible weak password change function is enabled, a warning prompt will be displayed if a user uses a weak password (containing less than 8 bytes or only digits, uppercase letters, or lowercase letters) during login or configuration. If both the forcible weak password change function and another password policy are enabled, the password will continue to be checked according to the other password policy during user login. If the password does not meet requirements of the other password policy, a prompt for changing the password will be displayed. The user is allowed to log in only after the new password meets requirements of the password policy.

The forcible weak password change function is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

Examples

The following example enables forcible weak password change.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy forced-password-modify
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **username** (Basic Configuration/Basic Management)

1.6 password policy printable-character-check

Function

Run the **password policy printable-character-check** command to enable the special character detection function.

Run the **no** form of this command to disable this feature.

Special character detection is disabled by default.

Syntax

password policy printable-character-check

no password policy printable-character-check

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After strong password detection and special character detection are configured, passwords that contain only special characters are invalid and cannot be configured successfully. Special characters include space, tilde (~), backtick (`), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent sign (%), caret (^), ampersand (&), asterisk (*), brackets (()), underscore (_), plus sign (+), minus sign (–), equal sign (=), braces ({}), vertical bar (|), square brackets ([]), backslash (\), colon (:), quotation mark ("), semicolon (;), apostrophe ('), angle brackets (<>), comma (,), period (.), and slash (/).

Examples

The following example enables special character detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy strong
Hostname(config)# password policy printable-character-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 service password-encryption

Function

Run the **service password-encryption** command to enable encrypted password storage.

Run the **no** form of this command to disable this feature.

Encrypted password storage is enabled by default.

Syntax

service password-encryption

no service password-encryption

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When encrypted password storage is disabled, all passwords used in the configuration process are displayed and stored in plaintext format unless the passwords are configured in ciphertext format. For security purposes, encrypted password storage should be enabled. When encrypted password storage is enabled and the **show running-config** command is run to display configurations or the **write** command is run to save configuration files, passwords configured by users are displayed in ciphertext format. If encrypted password storage is disabled again, passwords displayed in ciphertext format will not be restored to the plaintext format.

Examples

The following example enables encrypted password storage.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service password-encryption
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show password policy

Function

Run the **show password policy** command to display configured password security policies.

Syntax

show password policy

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display password security policies configured on a device.

Examples

The following example displays configured password security policies.

```
Hostname> enable
Hostname# show password policy
Global password policy configurations:
 Password encryption:              Enabled
 Password strong-check:            Enabled
Password secret-dictionary-check:   Enabled
 Password min-size:                Enabled (6 characters)
 Password life-cycle:              Enabled (90 days)
 Password no-repeat-times:          Enabled (max history record: 5)
```

Table 1-1 Output Fields of the show password policy Command

Field	Description
Password encryption	Whether passwords are stored in encrypted mode
Password strong-check	Whether strong password detection is enabled
Password secret-dictionary-check	Whether password dictionary check is enabled
Password min-size	Minimum password length
Password life-cycle	Password lifecycle
Password no-repeat-times	Number of latest configured passwords that cannot be used repeatedly

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 SSH Commands

Command	Function
clear ssh ip-block	Clear entries about blocked IP addresses and authentication failures.
crypto key generate	Generate the public key of the SSH server.
crypto key zeroize	Delete the public key of the SSH server.
disconnect ssh	Disconnect an established SSH client session.
disconnect ssh-session	Disconnect a suspended SSH client session.
ip scp client source-interface	Configure the source interface of the Secure copy protocol (SCP) client.
ip scp server enable	Enable the SCP server function.
ip scp server topdir	Configure the transmission path for uploading files to or downloading files from the SCP server.
ip ssh access-class	Configure an access control list (ACL) for the SSH server.
ip ssh authentication-retries	Configure the maximum number of user authentication attempts allowed on the SSH server.
ip ssh cipher-mode	Configure the encryption modes supported by the SSH server.
ip ssh compatible-ssh1x enable	Enable the SSHv1 function.
ip ssh hmac-algorithm	Configure the message authentication algorithms supported by the SSH server.
ip ssh ip-block disable	Disable the IP address blocking function of the SSH server.
ip ssh ip-block failed-times	Configure the number of authentication failures for blocking IP addresses and the time period for counting authentication failures on the SSH server.
ip ssh ip-block reactive	Configure the period for awakening blocked IP addresses.
ip ssh key-exchange	Configure the Diffie–Hellman (DH) key exchange algorithms supported by the SSH server.

ip ssh peer	Associate with the public key file and username of a client.
ip ssh port	Configure the listening port of the SSH server.
ip ssh source-interface	Configure the source interface of the SSH client.
ip ssh time-out	Configure the user authentication timeout time on the SSH server.
ip ssh version	Configure the SSH server version.
ipv6 ssh access-class	Configure an IPv6 ACL for the SSH server.
scp	Upload files to or download files from the remote SCP server.
show crypto key mypubkey	Display partial of the public key information of the SSH server.
show ip ssh	Display effective configurations of the SSH server.
show ssh	Display information about established SSH connections.
show ssh ip-block	Display information about blocked IP addresses and authentication failures.
show ssh-sessions	Display information about established SSH client sessions.
ssh	Establish an encrypted session with a remote network device.
ssh-session	Restore an established SSH client session.

1.1 clear ssh ip-block

Function

Run the **clear ssh ip-block** command to clear entries about blocked IP addresses and authentication failures.

Syntax

clear ssh ip-block { **all** | *ipv4-address* | *ipv6-address* }

Parameter Description

all: Clears all entries about blocked IP addresses and authentication failures.

ipv4-address: IPv4 source address based on which entries about blocked IP addresses and authentication failures are cleared.

ipv6-address: IPv6 source address based on which entries about blocked IP addresses and authentication failures are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The addresses and address description formats to be cleared can be obtained by running the **show ssh ip-block** command.

After entries about blocked IP addresses are cleared, these IP addresses are awakened immediately and can be used by Secure Shell (SSH) clients to log in to the device.

Examples

The following example clears all entries about blocked IP addresses and authentication failures.

```
Hostname> enable
Hostname# clear ssh ip-block all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 crypto key generate

Function

Run the **crypto key generate** command to generate the public key of the SSH server.

No public key is generated on the SSH server by default.

Syntax

crypto key generate { **dsa** | **ecc** | **rsa** }

Parameter Description

dsa: Generates a Digital Signature Algorithm (DSA) key.

ecc: Generates an Elliptic Curves Cryptography (ECC) key.

rsa: Generates a Rivest-Shamir-Adleman (RSA) key.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the SSH server service is required, run this command to generate the public key of the SSH server and run the **enable service ssh-server** command to enable the SSH server function. SSHv1 uses an RSA key, and SSHv2 uses an RSA or a DSA key. If an RSA key is generated, both SSHv1 and SSHv2 can use the key. If a DSA key is generated, only SSHv2 can use the key.

An SSH client uses only one of the ECC, DSA, and RSA public key algorithms for authentication in a connection. However, different clients support different public key algorithms. To ensure that clients can successfully log in to the server, you are advised to generate the ECC, DSA, and RSA key pairs on the server.

The minimum modulus length is 512 bits for the RSA host key and 360 bits for the DSA host key. The maximum modulus length of both is 2048 bits. In SSHv2, some clients (for example, the SCP clients) require that the length of the key generated on the server must be greater than or equal to 768 bits. When configuring RSA and DSA host keys, you are advised to set the host key modulus to 768 bits or larger.

The modulus length of an ECC host key can be 256, 384, or 512 bits, and the default modulus length is 512 bits.

You can run the **show crypto key mypubkey** command to check whether the public information about the RSA key exists. If yes, the RSA key has been generated.

Examples

The following example generates the RSA public key of the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# crypto key generate rsa
```

Notifications

When the RSA key of the SSH server is generated for the first time, the following notification will be displayed:

```
Hostname(config)#crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
// When the generation of the RSA key is successful, the following information will
be displayed:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
// When the generation of the RSA key fails, the following information will be displayed:
% Generating 512 bit RSA1 keys ...[fail]
% Generating 512 bit RSA keys ...[fail]
```

When the RSA key already exists on the server, the following notification will be displayed. If you select key replacement, you need to re-select the key bits, and information will be displayed, indicating whether the generation is successful. Otherwise, the configuration interface is closed.

```
Hostname(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:yes
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
```

When the entered number of RSA key bits is not within the range of 512 to 2048, the following notification will be displayed:

```
Hostname(config)#crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:360
sshd: rsa key in the range of 512 to 2048
How many bits in the modulus [512]:2590
sshd: bad data bits
How many bits in the modulus [512]:
```

Common Errors

An incorrect command is used to delete a key. The **no crypto key generate** command instead of the **crypto key zeroize** command is used to delete a key.

Platform Description

N/A

Related Commands

- **enable service** (System Configuration/Basic Management)

- crypto key zeroize

1.3 crypto key zeroize

Function

Run the **crypto key zeroize** command to delete the public key of the SSH server.

Syntax

crypto key zeroize { **dsa** | **ecc** | **rsa** }

Parameter Description

dsa: Deletes a DSA key.

ecc: Delete an ECC key.

rsa: Deletes an RSA key.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to delete the public key of the SSH server. After the public key is deleted, the SSH server state is **DISABLE**. To disable the SSH server, run the **no enable service ssh-server** command.

You can run the **show crypto key mypubkey** command to check whether the public information about the RSA key exists. If no, the RSA key has been deleted.

Examples

The following example deletes the RSA public key of the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# crypto key zeroize rsa
```

Notifications

When the RSA key already exists on the server, the following notification will be displayed:

```
Hostname(config)# crypto key zeroize rsa
% Keys to be removed
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]:yes
*Jan 16 06:52:57: %P17050-DEBUG: sshd: delete key file /rsa_private.bin
*Jan 16 06:52:57: %P17050-DEBUG: sshd: delete key file /rsa1_private.bin
```

When no RSA key is generated, the following notification will be displayed:

```
Hostname(config)# crypto key zeroize rsa
% The specified RSA keypair does not exist.
```

Common Errors

The **no** or **default** form of this command is used to delete a key.

Platform Description

N/A

Related Commands

- **show crypto key mypubkey**

1.4 disconnect ssh

Function

Run the **disconnect ssh** command to disconnect an established SSH client session.

Syntax

disconnect ssh { **vty** *session-id* | *session-id* }

Parameter Description

vty *session-id*: Specifies the Virtual Teletype (VTY) session ID of an SSH session to be disconnected. The value range is from 0 to 35.

session-id: Session ID of an SSH client session to be disconnected. The value range is from 0 to 35.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Serving as an SSH server, the device may connect to multiple SSH clients. You can run this command to forcibly disconnect a client from the device. The client disconnection methods are as follows:

- Specify an SSH session ID. To display the SSH session ID of a client, run the **show ssh** command.
- Specify a VTY session ID. To display the VTY session ID of a client, run the **show users** command. This command can be used to disconnect SSH connections only.

Examples

The following example disconnects the SSH client session whose session ID is 1.

```
Hostname> enable
Hostname# disconnect ssh 1
```

The following example disconnects the SSH client session whose VTY session ID is 1.

```
Hostname> enable
Hostname# disconnect ssh vty 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show users** (System Configuration/Line Configuration)

1.5 disconnect ssh-session

Function

Run the **disconnect ssh-session** command to disconnect a suspended SSH client session.

Syntax

disconnect ssh-session *session-id*

Parameter Description

session-id: Session ID of an SSH client session to be disconnected.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After the device connects to the SSH server as an SSH client, you can run the corresponding command to disconnect an SSH session with the specified session ID. To display information about the SSH connections established by the device as an SSH client, run the **show ssh-session** command.

Examples

The following example disconnects the SSH client session whose ID is 1.

```
Hostname> enable
Hostname# disconnect ssh-session 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ssh-session**

1.6 ip scp client source-interface

Function

Run the **ip scp client source-interface** command to configure the source interface of the Secure copy protocol (SCP) client.

Run the **no** form of this command to remove this configuration.

No SCP client source interface is configured by default. SSH packets use the packet sending source address queried based on the route as the source address by default.

Syntax

ip scp client source-interface *interface-type interface-number*

no ip scp client source-interface

Parameter Description

interface-type interface-number: Type and number of the SCP client source interface whose IP address is used as the global source address of the SCP client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used when the device serves as an SCP client. After the source interface is configured, the SCP client uses the IP address on the interface as the global source address during communication. If no source interface is configured, the source address of SCP packets will be obtained by querying the corresponding route based on the destination address. If no source interface or source IP address is independently specified for an SCP connection, the global configuration is used.

Examples

The following example configures Loopback 1 as the source interface of the SCP client and uses the IP address of Loopback 1 as the global source address of the SCP client.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip scp client source-interface loopback 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip scp server enable

Function

Run the **ip scp server enable** command to enable the SCP server function.

Run the **no** form of this command to disable this feature.

The SCP server function is disabled by default.

Syntax

ip scp server enable

no ip scp server enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the SCP server function is configured on the device, users can run the **scp** command to upload files to or download files from the device. Data exchanged during the process is encrypted for security. You can run the **show ip ssh** command to check whether the SCP server function is enabled.

Examples

The following example enables the SCP server function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip scp server enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable service ssh-server** (System Configuration/Basic Management)

1.8 ip scp server topdir

Function

Run the **ip scp server topdir** command to configure the transmission path for uploading files to or downloading files from the SCP server.

Run the **no** form of this command to remove this configuration.

The default transmission path for file upload and download is **flash:/**.

Syntax

ip scp server topdir { **flash:/***path* | **tmp:/***path* | **usb0:/***path* }

no ip scp server topdir

Parameter Description

flash /*path*: Selects the file transmission path from the extended flash space.

tmp /*path*: Sets the file transmission path to **tmp/vsd/**.

usb0 /*path*: Selects the file transmission path from Universal Serial Bus (USB) disk 0. This option is supported only when the device has one USB port with an extended USB flash drive inserted.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the transmission path for uploading and downloading files.

Examples

The following example sets the transmission path **tmp:/dir** for uploading files to and downloading files from the SCP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip scp server topdir tmp:/dir
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip ssh access-class

Function

Run the **ip ssh access-class** command to configure an access control list (ACL) for the SSH server.

Run the **no** form of this command to remove this configuration.

No ACL is configured on the SSH server by default.

Syntax

ip ssh access-class { *acl-name* | *acl-number* }

no ip ssh access-class

Parameter Description

acl-name: Name of a standard or an extended ACL used for the SSH server. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a standard or an extended ACL used for the SSH server. The value range is from 1 to 199 or from 1300 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to perform ACL filtering for all connections to the SSH server. In line mode, ACL filtering is performed only for specific lines. However, ACL filtering rules of the SSH server are effective to all SSH connections.

Examples

The following example configures ACL testv4 for the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh access-class testv4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip ssh authentication-retries

Function

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication attempts allowed on the SSH server.

Run the **no** form of this command to remove this configuration.

The default maximum number of authentication attempts allowed on the SSH server is **3**.

Syntax

ip ssh authentication-retries *retry-times*

no ip ssh authentication-retries

Parameter Description

retry-times: Maximum number of authentication attempts allowed. The value range is from 0 to 5.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of authentication attempts allowed on the SSH server. If authentication still does not succeed when the maximum number of user authentication attempts is reached, user authentication fails.

Examples

The following example sets the maximum number of authentication attempts allowed on the SSH server to **2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh authentication-retries 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ip ssh cipher-mode

Function

Run the **ip ssh cipher-mode** command to configure the encryption modes supported by the SSH server.

Run the **no** form of this command to remove this configuration.

The encryption modes supported by the SSH server are **ctr** and **gcm** by default.

Syntax

ip ssh cipher-mode { **cbc** | **ctr** | **gcm** | **others** } *

no ip ssh cipher-mode

Parameter Description

cbc: Configures the SSH server to support encryption mode cipher block chaining (CBC). The corresponding encryption algorithms are DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, and Blowfish-CBC.

ctr: Configures the SSH server to support encryption mode counter (CTR). The corresponding encryption algorithms are AES128-CTR, AES192-CTR, and AES256-CTR.

gcm: Configures the SSH server to support encryption mode Galois/Counter Mode (GCM), with Galois Message Authentication Code (GMAC). The corresponding encryption algorithms are AES128-GCM and AES256-GCM.

others: Configures the SSH server to support encryption mode "others". The corresponding encryption algorithm is RC4.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

SSHv1 supports encryption algorithms DES-CBC, 3DES-CBC, and Blowfish-CBC.

SSHv2 supports encryption algorithms AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, AES128-GCM, AES256-GCM, and RC4.

These algorithms can be grouped into four encryption modes: CBC, CTR, GCM (with GMAC), and others.

As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption modes supported by the SSH server to CTR and GCM to enhance the security level of the SSH server.

When the CBC, CTR, or GCM mode and algorithms supported in the mode are configured, the configuration result is still the original mode. For example, if **ip ssh cipher cbc 3des-cbc** is configured, the actual configuration result is the CBC mode.

Examples

The following example sets the encryption mode supported by the SSH server to the CTR mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh cipher-mode ctr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip ssh compatible-ssh1x enable

Function

Run the **ip ssh compatible-ssh1x enable** command to enable the SSHv1 function.

Run the **no** form of this command to disable this feature.

The SSHv1 function is disabled by default.

Syntax

ip ssh compatible-ssh1x enable

no ip ssh compatible-ssh1x enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the SSHv1 function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh compatible-ssh1x enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ip ssh hmac-algorithm

Function

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithms supported by the SSH server.

Run the **no** form of this command to remove this configuration.

SSHv1 servers do not support any message authentication algorithms, and SSHv2 servers support the MD5, SHA1, SHA1-96, MD5-96, sha2-256, and sha2-512 message authentication algorithms by default.

Syntax

ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }

no ip ssh hmac-algorith

Parameter Description

Md5:5: Sets the message authentication algorithm supported by the SSH server to MD5.

md5-96: Sets the message authentication algorithm supported by the SSH server to MD5-96.

sha1: Sets the message authentication algorithm supported by the SSH server to SHA1.

sha1-96: Sets the message authentication algorithm supported by the SSH server to SHA1-96.

sha2-256: Sets the message authentication algorithm supported by the SSH server to SHA2-256.

sha2-512: Sets the message authentication algorithm supported by the SSH server to SHA2-512.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the message authentication algorithm supported by the SSH server to SHA1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh hmac-algorithm sha1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ip ssh ip-block disable

Function

Run the **ip ssh ip-block disable** command to disable the IP address blocking function of the SSH server.

Run the **no** form of this command to enable this feature.

The IP address blocking function of the SSH server is enabled by default.

Syntax

ip ssh ip-block disable

no ip ssh ip-block disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the number of authentication failures for login through SSH reaches the configured limit in an authentication failure count period, the source IP address is blocked. That is, the SSH client that uses this

source IP address is not allowed to log in to the device to prevent the device being attacked. The SSH client can log in to the device only after the IP address is awakened.

Examples

The following example disables the IP address blocking function on the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh ip-block disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ip ssh ip-block failed-times

Function

Run the **ip ssh ip-block failed-times** command to configure the number of authentication failures for blocking IP addresses and the time period for counting authentication failures on the SSH server.

Run the **no** form of this command to remove this configuration.

The allowed maximum number of authentication failures is **6**, and the time period for counting authentication failures is **5** minutes by default.

Syntax

ip ssh ip-block failed-times *failed-times* **period** *period-time*

no ip ssh ip-block failed-times *failed-times* **period** *period-time*

Parameter Description

failed-times: Number of authentication failures for blocking IP addresses. The value range is from 1 to 10.

period-time: Time period for counting authentication failures, in minutes. The value range is from 1 to 120.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the IP address blocking function is enabled, if the number of consecutive authentication failures for device login through SSH reaches the configured limit in an authentication failure count period, the source IP address is blocked. If the number of consecutive authentication failures does not reach the configured limit in an authentication failure count period, or one authentication is successful, the authentication failures are cleared.

Examples

The following example sets the number of authentication failures for blocking IP addresses to 3 and the time period for counting authentication failures to 3 minutes on the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh ip-block failed-times 3 period 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ip ssh ip-block reactive

Function

Run the **ip ssh ip-block reactive** command to configure the period for awakening blocked IP addresses.

Run the **no** form of this command to remove this configuration.

Blocked IP addresses are awakened every **5** minutes by default.

Syntax

ip ssh ip-block reactive *reactive-interval*

no ip ssh ip-block reactive

Parameter Description

reactive-interval: Period for awakening blocked IP addresses. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the time period for awakening the blocked source IP address reaches, the entry with the blocked source IP address is cleared. An SSH client can use this IP address to log in to the device.

Examples

The following example sets the time period for awakening blocked IP addresses on the SSH server to 3 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh ip-block reactive 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip ssh key-exchange

Function

Run the **ip ssh key-exchange** command to configure the Diffie–Hellman (DH) key exchange algorithms supported by the SSH server.

Run the **no** form of this command to remove this configuration.

Ruijie SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521 for key exchange, and SSHv1 servers support none by default.

Syntax

ip ssh key-exchange { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** | **ecdh_sha2_nistp256** | **ecdh_sha2_nistp384** | **ecdh_sha2_nistp521** }

no ip ssh key-exchange

Parameter Description

dh_group_exchange_sha1: Sets the DH key exchange algorithm to diffie-hellman-group-exchange-sha1. The default key length is **2048** bytes, which is not configurable.

dh_group14_sha1: Sets the DH key exchange algorithm to diffie-hellman-group14-sha1. The key length is 2048 bytes.

dh_group1_sha1: Sets the DH key exchange algorithm to diffie-hellman-group1-sha1. The key length is 1024 bytes.

ecdh_sha2_nistp256: Sets the DH key exchange algorithm to ecdh_sha2_nistp256. The key length is 256 bytes.

ecdh_sha2_nistp384: Sets the DH key exchange algorithm to ecdh_sha2_nistp384. The key length is 384 bytes.

ecdh_sha2_nistp521: Sets the DH key exchange algorithm to ecdh_sha2_nistp521. The key length is 512 bytes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The SSHv1 server does not support any DH key exchange algorithm. The SSHv2 server supports the following DH key exchange algorithms: diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521. You can select DH key exchange algorithms supported by the SSH server as required.

Examples

The following example sets the DH key exchange algorithm supported by the SSH server to diffie-hellman-group14-sha1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh key-exchange dh_group14_sha1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip ssh peer

Function

Run the **ip ssh peer** command to associate with the public key file and username of a client.

Run the **no** form of this command to remove this configuration.

Syntax

ip ssh peer *username* **public-key** { **dsa** | **ecc** | **rsa** } *filename-path*

no ip ssh peer *username* **public-key** { **rsa** | **dsa** | **ecc** }

Parameter Description

username: Username of a client.

dsa: Sets the public key type to DSA.

ecc: Sets the public key type to ECC.

rsa: Sets the public key type to RSA.

filename-path: Path where the public key file is stored.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example associates username **test** with the RSA public key file **flash:rsa.pub**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh peer test public-key rsa flash:rsa.pub
```

Notifications

When the number of associated public key files exceeds the maximum value 1024, the following notification will be displayed:

```
Hostname(config)# ip ssh peer test public-key rsa flash:rsa.pub
%% Too many public-keys, system support max public key 1024
```

When the name of the associated public key file is not entered, the following notification will be displayed:

```
Hostname(config)#ip ssh peer test public-key rsa flash:
% Invalid file name
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ip ssh port

Function

Run the **ip ssh port** command to configure the listening port of the SSH server.

Run the **no** form of this command to remove this configuration.

The default listening port of the SSH server is port **22**.

Syntax

ip ssh port *ssh-monitor-port*

no ip ssh port

Parameter Description

ssh-monitor-port: Listening port of the SSH server. The value range is from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the listening port of the SSH server to **10000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh port 10000
```

Notifications

When the configured port is the same as the current value, the following notification will be displayed:

```
Hostname(config)# ip ssh port 22
% SSH tcp-port has been 22
```

When a port in the listening state is configured as the listening port of the SSH server, the following notification will be displayed:

```
Hostname(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port,otherwise the system
will use the old tcp-port(22)!
```

When an error occurs after the configured listening port starts listening, the following notification will be displayed:

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

When a listening port is successfully configured, the following notification will be displayed:

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip ssh source-interface

Function

Run the **ip ssh source-interface** command to configure the source interface of the SSH client.

Run the **no** form of this command to remove this configuration.

No SSH client source interface is configured by default.

Syntax

ip ssh source-interface *interface-type interface-number*

no ip ssh source-interface

Parameter Description

interface-type interface-number: Type and number of the SSH client source interface whose IP address is used as the global source address of the SSH client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to specify the source interface when the device serves as an SSH client, and the IP address of which will be used as the global source address of the SSH client. When the **ssh** command is used to connect to an SSH server, this global configuration will be used if no source interface or source address is specified for this connection. When no SSH client source interface is configured, SSH packets use the packet sending source address queried based on the route as the source address.

Examples

The following example configures Loopback 1 as the source interface of an SSH client.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh source-interface loopback 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip ssh time-out

Function

Run the **ip ssh time-out** command to configure the user authentication timeout time on the SSH server.

Run the **no** form of this command to remove this configuration.

The default user authentication timeout time on the SSH server is **120** seconds.

Syntax

ip ssh time-out *timeout-time*

no ip ssh time-out

Parameter Description

timeout-time: User authentication timeout time, in seconds. The value range is from 1 to 120.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the user authentication timeout time on the SSH server. The SSH server starts the timer after receiving a user connection request. If authentication does not succeed after 120 seconds, authentication fails.

Examples

The following example sets the user authentication timeout time on the SSH server to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh time-out 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip ssh version

Function

Run the **ip ssh version** command to configure the SSH server version.

Run the **no** form of this command to remove this configuration.

The SSH server is compatible with the SSHv1 and SSHv2 clients by default.

Syntax

ip ssh version *version-type*

no ip ssh version

Parameter Description

version-type: Version of the SSH server. The value is 1 or 2. The value **1** indicates that the SSH server supports only connection requests from SSHv1 clients, and the value **2** indicates that the SSH server supports only connection requests from SSHv2 clients.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the version supported by the SSH server. If the *version-type* parameter is not specified, the SSH server is compatible with SSHv1 and SSHv2 clients. That is, both SSHv1 and SSHv2 clients can connect to the SSH server. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Examples

The following example sets the version supported by the SSH server to SSHv2 only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh version 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ipv6 ssh access-class

Function

Run the **ipv6 ssh access-class** command to configure an IPv6 ACL for the SSH server.

Run the **no** form of this command to remove this configuration.

No IPv6 ACL is configured on the SSH server by default.

Syntax

ipv6 ssh access-class *acl-name*

no ipv6 ssh access-class

Parameter Description

acl-name: Name of an IPv6 ACL used for the SSH server.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to perform IPv6 ACL filtering for all connections to the SSH server. In line mode, IPv6 ACL filtering is performed only for specific lines. However, IPv6 ACL filtering rules of the SSH server are effective to all SSH connections.

Examples

The following example configures IPv6 ACL **testv6** for the SSH server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 ssh access-class testv6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 scp

Function

Run the **scp** command to upload files to or download files from the remote SCP server.

Syntax

scp [**oob**] [**-v** { **1** | **2** } | **-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** } | **-p** *port-num*] * *source-file destination-file* [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }] [**/vrf** *vrf-name*]

Parameter Description

oob: Connects to the remote SCP server through out-of-band communication (over the MGMT port typically). This option is valid only when the device has an MGMT port.

-**v** { **1 | 2** }: Configures the SSH version. The value **1** indicates SSHv1, and the value **2** indicates SSHv2. If this parameter is not specified, SSHv2 is used.

-c: Configures the data encryption algorithm. During algorithm negotiation, the SSH client sends only the user-specified encryption algorithm to the server. If the server does not support the user-specified encryption algorithm, the server closes the SSH connection. If this parameter is not specified, the SSH client sends all supported algorithms to the server during algorithm negotiation.

-**c 3des**: Sets the data encryption algorithm to 3DES.

-**c aes128-cbc**: Sets the data encryption algorithm to AES128-CBC (128-bit key).

-**c aes192-cbc**: Sets the data encryption algorithm to AES192-CBC (192-bit key).

-**c aes256-cbc**: Sets the data encryption algorithm to AES256-CBC (256-bit key).

-**c aes128-ctr**: Sets the data encryption algorithm to AES128-CTR (128-bit key).

-**c aes192-ctr**: Sets the data encryption algorithm to AES192-CTR (192-bit key).

-**c aes256-ctr**: Sets the data encryption algorithm to AES256-CTR (256-bit key).

-**c aes128-gcm**: Sets the data encryption algorithm to AES128-GCM (128-bit key).

-**c aes256-gcm**: Sets the data encryption algorithm to AES256-GCM (256-bit key).

-m: Configures the hash-based message authentication code (HMAC) algorithm. During algorithm negotiation, the SCP client sends only the user-specified HMAC algorithm to the server. If the server does not support the user-specified HMAC algorithm, the server closes the SSH connection. If this parameter is not specified, the SSH client sends all supported algorithms to the server during algorithm negotiation. Supported algorithms include hmac-md5-96, hmac-md5-128, hmac-sha1-96, hmac-sha1-160, hmac-sha2-256, and hmac-sha2-512.

-p *port-num*: Configures the destination port in packets sent from the client to the server. The value range is from 0 to 65535. If this parameter is not specified, the destination port is port 22.

source-file destination-file: File copied to the destination path, which can be from the remote server to the device or from the device to the remote server. *source-file* indicates the path where the source file is stored. *destination-file* indicates the path where a file is copied to. Files on the remote server are displayed in *username*@host:/*filename* format, and files on the device are displayed in *path*:/*filename* format. The formats are as follows:

- flash:/filename: Extended flash space.
- usb0:/filename: Extended USB disk 0. This option is supported when the device has one USB port with a USB flash drive inserted.
- tmp:/filename: Temporary tmp/vsd/ directory.

via *mgmt-name*: Specifies the MGMT port used by the SSH server when the oob option is specified.

/source: Specifies the source IP address or interface used by an SCP client.

ip *ipv4-address*: Specifies the source IPv4 address used by an SCP client.

ipv6 *ipv6-address*: Specifies the source IPv6 address used by an SCP client.

interface *interface-type interface-number*: Specifies the source interface used by an SCP client.

/vrf *vrf-name*: Specifies the virtual routing and forwarding (VRF) routing table to be displayed.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

When the device serves as an SCP client, the device can run the **scp** command to establish a connection to the SCP server to upload files to and download files from the SCP server.

SSHv1 does not support the HMAC algorithm. If both SSHv1 and the HMAC algorithm are specified, the HMAC configuration will be ignored.

Examples

The following example downloads the **config.text** file from a remote SCP server whose IP address is 192.168.23.122 to the local device using username **admin** and saves the file as **flash:/config.text**.

```
Hostname> enable
Hostname#scp admin@192.168.23.122:/config.text flash:/config.text
```

The following example uploads the **flash:/config.text** file from the local device to the remote SCP server whose IP address is 192.168.23.122 using username **admin** and saves the file as **config.text**.

```
Hostname> enable
Hostname# scp flash:/config.text admin@192.168.23.122:/config.text
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 show crypto key mypubkey

Function

Run the **show crypto key mypubkey** command to display partial of the public key information of the SSH server.

Syntax

show crypto key mypubkey { **dsa** | **ecc** | **rsa** }

Parameter Description

dsa: Displays the DSA key information.

ecc: Displays the ECC key information.

rsa: Displays the RSA key information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the public key information of the SSH server, including the key generation time, key name, and partial of key content.

Examples

The following example displays partial RSA key information of the SSH server.

```
Hostname> enable
Hostname# show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
 Key name: RSA1 private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
       AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q10kz+4/
       /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
 Key name: RSA private
 Usage: SSH Purpose Key
 Key is not exportable.
```

```
Key Data:
       AAAAAwEA AQAAAEEA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3
       LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OAkQ==
```

Table 1-1 Output Fields of the show crypto key mypubkey Command

Field	Description
Key pair was generated at	Key generation time
Key name	Key name
Usage	Key use description
Key Data	Partial of public key content

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 show ip ssh

Function

Run the **show ip ssh** command to display effective configurations of the SSH server.

Syntax

show ip ssh

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display effective configurations of the SSH server, including the version, whether the SSH server function is enabled, port number, encryption mode, message authentication algorithm, authentication timeout time, and maximum number of authentication attempts allowed.

If an SSH version is configured but the corresponding server key is not generated, a message indicating that the SSH version is unavailable will be displayed.

Examples

The following example displays effective configurations of the SSH server when the SSH server and SCP server functions are disabled.

```
Hostname> enable
Hostname# show ip ssh
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
SSH Port:             22
SSH Cipher Mode:       cbc,ctr,others
SSH HMAC Algorithm:    md5-96,md5,sha1-96,sha1
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:        disabled
SSH dh-exchange min-len: 2048
SSH ip-block:          disabled
```

The following example displays effective configurations of the SSH server when the SSH server and SCP server functions are enabled.

```
Hostname> enable
Hostname# show ip ssh
SSH Enable - version 1.99
SSH Port:             22
SSH Cipher Mode:       cbc,ctr,others
SSH HMAC Algorithm:    md5-96,md5,sha1-96,sha1
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:        enabled
SSH dh-exchange min-len: 2048
SSH ip-block:          enabled
```

Table 1-2 Output Fields of the show ip ssh Command

Field	Description
SSH Enable/Disable	Whether the SSH server function is enabled
version 1|2	SSH version supported by the SSH server
please generate rsa and dsa key to enable SSH	Whether the RSA/DSA public key is generated to enable the SSH server function
SSH Port	Listening port of the SSH server
SSH Cipher Mode	Encryption mode of the SSH server
SSH HMAC Algorithm	Message authentication algorithm of the SSH server

Field	Description
Authentication timeout	User authentication timeout time
Authentication retries	Maximum number of authentication attempts allowed
SSH SCP Server enabled/disabled	Whether the SSH SCP server function is enabled
SSH dh-exchange min-len	Minimum key length negotiated by the key exchange algorithm of the SSH server
SSH ip-block enabled/disabled	Whether the IP address blocking function is enabled on the SSH server

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 show ssh

Function

Run the **show ssh** command to display information about established SSH connections.

Syntax

show ssh

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about established SSH connections, including the VTY number occupied by a connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and username.

Examples

The following example displays information about established SSH connections.

```
Hostname> enable
Hostname# show ssh
Connection Version Encryption      Hmac        Compress   State          Username
       0    1.5 blowfish                    zlib      Session started test
       1    2.0 aes256-cbc      hmac-sha1    zlib      Session started test
```

Table 1-3 Output Fields of the show ssh Command

Field	Description
Connection	VTY number occupied by a connection
Version	SSH version supported by an SSH client
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compression algorithm
State	Connection status
Username	Username

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 show ssh ip-block

Function

Run the **show ssh ip-block** command to display information about blocked IP addresses and authentication failures.

Syntax

show ssh ip-block { **all** | **list** }

Parameter Description

all: Displays information about all blocked IP addresses and authentication failures.

list: Displays information about blocked IP addresses.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about all blocked IP addresses and authentication failures. Blocked IP address information includes the source IPv4 or IPv6 addresses and remaining time for awakening blocked IP addresses. Authentication failure information includes the source IPv4 or IPv6 addresses, status, and number of authentication failures.

Examples

The following example displays information about all blocked IP addresses and authentication failures.

```
Hostname> enable
Hostname# show ssh ip-block all
------------------------
IP Address                              State      Auth-fail Count
------------------------
172.30.31.16                            AUTH FAILED    3
172.30.31.17                            BLOCKED        6
------------------------
```

Table 1-4 Output Fields of the show ssh ip-block all Command

Field	Description
IP Address	Source IPv4 or IPv6 address
State	Status ● **AUTH FAILED**: Authentication fails but the blocking conditions are not met. ● **BLOCKED**: Blocking conditions are met.
Auth-fail Count	Number of authentication failures

The following example displays information about blocked IP addresses.

```
Hostname> enable
Hostname# show ssh ip-block list
------------------------
IP Address                              UnBlock Interval (Seconds)
------------------------
172.30.31.17                            296
------------------------
```

Table 1-5 Output Fields of the show ssh ip-block list Command

Field	Description
IP Address	Source IPv4 or IPv6 address

Field	Description
UnBlock Interval (Seconds)	Remaining time for awakening blocked IP addresses, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show ssh-sessions

Function

Run the **show ssh-sessions** command to display information about established SSH client sessions.

Syntax

show ssh-sessions

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about established SSH client sessions, including the VTY number occupied by a connection, SSH version, and server address.

Examples

The following example displays information about established SSH client sessions.

```
Hostname> enable
Hostname# show ssh-sessions
Connect No.  SSH Version Server Address
-----  -----  ----
0          2.0        192.168.23.122
1          1.5        192.168.23.122
```

Table 1-6 Output Fields of the show ssh-sessions Command

Field	Description
Connect No.	Client No.
SSH Version	SSH version of a session
Server Address	IP address of the remote SSH server

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 ssh

Function

Run the **ssh** command to establish an encrypted session with a remote network device.

Syntax

ssh [**oob**] [**-v** { **1** | **2** } | **-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **-l** *username* | **-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** } | **-p** *port-num*] * { *ip-address* | *hostname* } [**via** *mgmt-name*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }] [**/vrf** *vrf-name*]

Parameter Description

oob: Connects to the remote SSH server through out-of-band communication (over the MGMT port typically). This option is valid only when the device has an MGMT port.

-**v** { **1 | 2** }: Configures the SSH version. The value **1** indicates SSHv1, and the value **2** indicates SSHv2. If this parameter is not specified, SSHv2 is used.

-c: Configures the data encryption algorithm. During algorithm negotiation, the SSH client only sends the user-specified encryption algorithm to the server. If the server does not support the user-specified encryption algorithm, the server closes the SSH connection. If this parameter is not specified, the SSH client sends all supported algorithms to the server during algorithm negotiation.

-**c 3des**: Sets the data encryption algorithm to 3DES.

-**c aes128-cbc**: Sets the data encryption algorithm to AES128-CBC (128-bit key).

-**c aes192-cbc**: Sets the data encryption algorithm to AES192-CBC (192-bit key).

-**c aes256-cbc**: Sets the data encryption algorithm to AES256-CBC (256-bit key).

-**c aes128-ctr**: Sets the data encryption algorithm to AES128-CTR (128-bit key).

-**c aes192-ctr**: Sets the data encryption algorithm to AES192-CTR (192-bit key).

-**c aes256-ctr**: Sets the data encryption algorithm to AES256-CTR (256-bit key).

-**c aes128-gcm**: Sets the data encryption algorithm to AES128-GCM (128-bit key).

-**c aes256-gcm**: Sets the data encryption algorithm to AES256-GCM (256-bit key)

-l *username*: Specifies the username used for login.

-m: Configures the HMAC algorithm. During algorithm negotiation, the SCP client sends only the user-specified HMAC algorithm to the server. If the server does not support the user-specified HMAC algorithm, the server closes the SSH connection. If this parameter is not specified, the SSH client sends all supported algorithms to the server during algorithm negotiation. Supported algorithms include hmac-md5-96, hmac-md5-128, hmac-sha1-96, hmac-sha1-160, hmac-sha2-256, and hmac-sha2-512.

-p *port-num*: Configures the destination port in packets sent from the client to the server. The value range is from 0 to 65535. If this parameter is not specified, the destination port is port 22.

ip-address: IPv4/IPv6 address of the remote server.

hostname: IPv4/IPv6 host name of the remote server.

via *mgmt-name*: Specifies the MGMT port used by the SSH server when the oob option is configured.

/source: Specifies the source IP address or interface used by an SCP client.

ip *ipv4-address*: Specifies the source IPv4 address used by an SCP client.

ipv6 *ipv6-address*: Specifies the source IPv6 address used by an SCP client.

interface *interface-type interface-number*: Specifies the source interface used by an SCP client.

/vrf *vrf-name*: Specifies the virtual routing and forwarding (VRF) routing table to be displayed.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

When the device serves as an SSH client, the device can run the **ssh** command to establish a connection to the SSH server. This connection is similar to but more secure than a Telnet connection due to the authentication and encrypted transmission features. Different versions support different parameters. During parameter configuration, note the following:

- SSHv1 supports only the DES (56-bit key) and 3DES (168-bit key) encryption algorithms.
- SSHv2 supports the following Advanced Encryption Standards (AES): AES128-CBC, AES192-CBC, AES256-CBC, AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, and AES256-GCM.
- SSHv1 does not support the HMAC algorithm.
- If you specify an unmatched encryption or authentication algorithm when selecting an SSH version, the unmatched algorithm will be ignored when a connection is established.

Examples

The following example uses username **admin** to log in to a device that provides the SSH server service and whose IP address is 192.168.23.122 through SSH.

```
Hostname> enable
Hostname# ssh -l admin 192.168.23.122
```

The following example uses username **admin** to log in to a device that provides the SSH server service and whose IP address is 192.168.23.122 through SSHv2. The encryption algorithm is set to **aes128-cbc**, and the authentication algorithm is set to **hmac-md5-128**.

```
Hostname> enable
Hostname# ssh -v 2 -c aes128-cbc  -m hmac-md5-128 -l admin 192.168.23.122
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 ssh-session

Function

Run the **ssh-session** command to restore an established SSH client session.

Syntax

ssh-session *session-id*

Parameter Description

session-id: ID of an established SSH client session.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After the device establishes an SSH session with the SSH server as a client, you can press Ctrl+Shift+6+X to exit the session temporarily. After exiting the session, you can run the corresponding command to restore the session.

Examples

The following example restores the SSH client session whose session ID is 1.

```
Hostname> enable
Hostname# ssh-session 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Global IP-MAC Address Binding Commands

Command	Function
address-bind	Configure a global IP-Media Access Control (MAC) address binding policy.
address-bind binding-filter logging	Enable address binding log filtering.
address-bind install	Enable the IP-MAC address binding function.
address-bind ipv6-mode	Configure the IPv6 address binding mode.
address-bind uplink	Configure a port as an excluded port for address binding.
show address-bind	Display the global IP-MAC address binding policy.
show address-bind uplink	Display excluded ports for address binding.

1.1 address-bind

Function

Run the **address-bind** command to configure a global IP-Media Access Control (MAC) address binding policy.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IP-MAC address binding policy is configured by default.

Syntax

address-bind { *ipv4-address mac-address* | *ipv6-address mac-address* }

no address-bind { *ipv4-address mac-address* | *ipv6-address mac-address* }

default address-bind { *ipv4-address mac-address* | *ipv6-address mac-address* }

Parameter Description

ipv4-address mac-address: IPv4-MAC address binding.

ipv6-address mac-address: IPv6-MAC address binding.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a global IPv4-MAC address binding policy with the IPv4 address being 192.168.5.1 and the MAC address being 00d0.f800.0001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 address-bind binding-filter logging

Function

Run the **address-bind binding-filter logging** command to enable address binding log filtering.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Address binding log filtering is disabled by default.

Syntax

address-bind binding-filter logging [**rate-limit** *rate*]

no address-bind binding-filter logging

default address-bind binding-filter logging

Parameter Description

rate-limit *rate*: Specifies the rate for printing global IPv4-MAC address binding logs, in pieces per minutes. The value range is from 1 to 120. The default value is **10**. If this parameter is not specified, address binding log filtering is enabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the address binding log filtering function is enabled, the device prints alert logs for IP packets that do not contain bound IP address and MAC address.

When the printing rate of address binding logs exceeds the configured rate, the number of suppressed logs is displayed.

Examples

The following example enables the address binding log filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-bind binding-filter logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 address-bind install

Function

Run the **address-bind install** command to enable the IP-MAC address binding function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The IP-MAC address binding function is disabled by default.

Syntax

address-bind install

no address-bind install

default address-bind install

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After IP-MAC address binding is enabled, the device forwards packets based on the IP-MAC address binding policy.

Before enabling this function, you need to run the **address-bind** command to configure a global IP-MAC address binding policy or run the **address-bind uplink** command to configure the port on the device used to connect to the user host as an excluded port. Otherwise, the connection may be interrupted.

Examples

The following example enables the IP-MAC address binding function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001
Hostname(config)# address-bind install
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- address-bind
- address-bind uplink

1.4 address-bind ipv6-mode

Function

Run the **address-bind ipv6-mode** command to configure the IPv6 address binding mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default IPv6 address binding mode is the strict mode.

Syntax

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

no address-bind ipv6-mode

default address-bind ipv6-mode

Parameter Description

compatible: Specifies the compatible mode.

loose: Specifies the loose mode.

strict: Specifies the strict mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Table 1-1 describes the forwarding rules in different IPv6 address binding modes.

Table 1-1 Forwarding Rules

Binding Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the IPv4-MAC address binding conditions are forwarded.	Packets matching the IPv6-MAC address binding conditions are forwarded.

Binding Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Loose	Packets matching the IPv4-MAC address binding conditions are forwarded.	• If IPv6-MAC address binding is configured, packets matching the IPv6-MAC address binding conditions are forwarded. • If IPv6-MAC address binding is not configured, all IPv6 packets are forwarded.
Compatible	Packets matching the IPv4-MAC address binding conditions are forwarded.	• IPv6 packets are forwarded if they contain MAC addresses matching the MAC address in the IPv4-MAC address binding policy. • Packets matching the IPv6-MAC address binding conditions are forwarded.

Examples

The following example sets the IPv6 address binding mode to the compatible mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-bind ipv6-mode compatible
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 address-bind uplink

Function

Run the **address-bind uplink** command to configure a port as an excluded port for address binding.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No port is configured as an excluded port for address binding by default.

Syntax

address-bind uplink *interface-type interface-number*

no address-bind uplink *interface-type interface-number*

default address-bind uplink *interface-type interface-number*

Parameter Description

interface-type interface-number: Type and number of a port configured as an excluded port. The port types include switching ports and layer 2 (L2) aggregation ports (APs).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures GigabitEthernet 0/1 as an excluded port for address binding.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# address-bind uplink gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show address-bind

Function

Run the **show address-bind** command to display the global IP-MAC address binding policy.

Syntax

show address-bind

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the global IP-MAC address binding policy.

```
Hostname> enable
Hostname# show address-bind
Total Bind Addresses in System : 2
IpAddress         BindingMacAddr
192.168.5.1       00d0.f800.0001
1:1::1           00d0.f800.0002
```

Table 1-2 Output Fields of the show address-bind Command

Field	Description
Total Bind Addresses in System	Number of global IPv4-MAC address bindings configured on the device
IpAddress	Bound IP address
BindingMacAddr	Bound MAC address

Notifications

N/A

Platform Description

N/A

Related Commands

- address-bind

1.7 show address-bind uplink

Function

Run the **show address-bind uplink** command to display excluded ports for address binding.

Syntax

show address-bind uplink

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays excluded ports for address binding.

```
Hostname> enable
Hostname# show address-bind uplink
Port      State
Gi0/1     Enabled
Default    Disabled
```

Table 1-3 Output Fields of the show address-bind uplink Command

Field	Description
Port	Excluded port. No port is an excluded port by default.
State	Whether a port is an excluded port. **Enabled** indicates that a port is an excluded port, and **Disabled** indicates that a port is not an excluded port.

Notifications

N/A

Platform Description

N/A

Related Commands

- **address-bind uplink**

1 Port Security Commands

Command	Function
switchport port-security	Enable the port security function.
switchport port-security aging	Configure the secure address aging time and its application scope on a port.
switchport port-security binding	Configure the secure addresses bound to a port.
switchport port-security binding-filter logging	Enable address binding log filtering and configure the log printing rate.
switchport port-security interface binding	Configure security binding for a port.
switchport port-security mac-address	Configure static secure addresses.
switchport port-security interface mac-address	Configure static secure addresses.
switchport port-security maximum	Configure the maximum number of secure addresses for a port.
switchport port-security mac-address sticky	Enable sticky MAC address learning and configure sticky MAC addresses.
switchport port-security violation	Configure the method for handling packets that violate the port security requirements.
show port-security	Display port security configurations and secure addresses.

1.1 switchport port-security

Function

Run the **switchport port-security** command to enable the port security function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The port security function is disabled by default.

Syntax

switchport port-security

no switchport port-security

default switchport port-security

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The port security function strictly controls Media Access Control (MAC) addresses and IP addresses (optional) that can access a port.

The port security function can be configured only on switching ports and layer 2 (L2) aggregation ports (APs). Ports configured with port security are called secure ports. If a secure address is configured for a secure port, the secure port allows only packets whose source address is the configured secure address to pass through. Other packets are discarded.

Examples

The following example enables port security on Gigabitethernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 switchport port-security aging

Function

Run the **switchport port-security aging** command to configure the secure address aging time and its application scope on a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The secure address aging time is **0** (that is, not aged), and the aging time applies only to dynamically learned addresses by default.

Syntax

switchport port-security aging { **static** | **time** *aging-time* }

no switchport port-security aging { **static** | **time** }

default switchport port-security aging { **static** | **time** }

Parameter Description

static: Applies the configured aging time to manually configured and dynamically learned addresses.

time *aging-time*: Configures the aging time of all secure addresses on a port, in minutes. The value range is from 0 to 1440. When the aging time is set to **0**, secure addresses on a port will not be aged.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command together with the **switchport port-security maximum** command for configuring the maximum number of secure addresses allow the device to automatically add and delete secure addresses on a port.

When the **no switchport port-security aging time** command is run to restore the secure address aging time on a port to **0**, secure address aging is disabled on the port. The **no switchport port-security aging static** command allows the aging time to be applied only to dynamically learned secure addresses.

When port security and 802.1x authentication are both enabled but the secure address has aged, 802.1x users must re-initiate authentication requests to continue the communication.

Examples

The following example sets the aging time of secure addresses on GigabitEthernet 0/1 to 8 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# switchport port-security aging time 8
Hostname(config-if)# switchport port-security aging static
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **switchport port-security maximum**

1.3 switchport port-security binding

Function

Run the **switchport port-security binding** command to configure the secure addresses bound to a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No secure address is bound to a port by default.

Syntax

switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

default switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

Parameter Description

mac-address: Source MAC address to be bound to a port, VLAN ID, and IP address.

vlan *vlan-id*: Specifies the virtual local area network (VLAN) ID to be bound to a port, source MAC address, and IP address. The value range is from 1 to 4094.

ipv4-address: IPv4 address to be bound to a port.

ipv6-address: IPv6 address to be bound to a port.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You must first enter the interface configuration mode of the port to be bound and then run this command to bind the port with the source MAC address (optional), VLAN ID (optional), and IP address. Only packets match the security binding can enter the device, and other packets will be discarded.

Packets that comply with IP-MAC address binding or IP address binding for port security can be forwarded only when their source MAC address is the secure address bound to the port.

Before dynamically learned secure addresses are added to the secure address table, packets that comply with IP-MAC address binding or IP address binding for port security cannot be forwarded.

Static secure addresses can access the Internet without authentication. If authorization exists, only static secure addresses that comply with the authorization binding can access the Internet.

Examples

The following example binds IPv4 address 192.168.1.100 to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security binding
192.168.1.100
```

The following example binds IPv4 address 192.168.1.100, MAC address 00d0.f800.5555, and VLAN 1 to GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security binding
00d0.f800.5555 vlan 1 192.168.1.100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 switchport port-security binding-filter logging

Function

Run the **switchport port-security binding-filter logging** command to enable address binding log filtering and configure the log printing rate.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Address binding log filtering is disabled by default.

Syntax

switchport port-security binding-filter logging [**rate-limit** *rate*]

no switchport port-security binding-filter logging

default switchport port-security binding-filter logging

Parameter Description

rate-limit *rate*: Configures the rate for printing security binding logs, in pieces per second. The value range is from 1 to 120. The default value is **10**. If this parameter is not specified, address binding log filtering is enabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the binding log filtering function is enabled, the device prints alert logs if received IP packets do not match the bound IP and MAC addresses or the bound IP address for port security.

When the binding log printing rate exceeds the configured rate, the number of suppressed logs will be displayed.

Examples

The following example enables the binding log filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security binding-filter logging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 switchport port-security interface binding

Function

Run the **switchport port-security interface binding** command to configure security binding for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No security binding is configured by default.

Syntax

switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

default switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number of the bound port.

mac-address: Bound source MAC address.

vlan *vlan-id*: Specifies the VLAN bound to the source MAC address.

ipv4-address: Bound IPv4 address.

ipv6-address: Bound IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to bind a port with a source MAC address (optional), VLAN ID (optional), and IP address as the security binding of the port. Only packets match the security binding can enter the device, and other packets will be discarded.

Unlike the **switchport port-security binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* } command, this command can be directly configured in global configuration mode without needing to enter the interface configuration mode of the bound port.

Packets that comply with IP-MAC address binding or IP address binding for port security can be forwarded only when their source MAC address is the secure address bound to the port.

Before dynamically learned secure addresses are added to the secure address table, packets that comply with IP-MAC address binding or IP address binding for port security cannot be forwarded.

Examples

The following example binds GigabitEthernet 0/1 to IPv4 secure address 192.168.1.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 binding
192.168.1.100
```

The following example binds GigabitEthernet 0/1 to MAC address 00d0.f800.5555, VLAN ID 1, and IPv4 secure address 192.168.1.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 binding
00d0.f800.5555 vlan 1 192.168.1.100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 switchport port-security mac-address

Function

Run the **switchport port-security mac-address** command to configure static secure addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static secure address is configured by default.

Syntax

switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

no switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

default switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

Parameter Description

mac-address *mac-address*: Specifies the static secure address to be configured.

vlan *vlan-id*: Specifies the VLAN to which a MAC address belongs. The value range is from 1 to 4094. This parameter takes effect only for trunk ports.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the static secure address to 00d0.f800.5555 and VLAN ID to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
00d0.f800.5555 vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 switchport port-security interface mac-address

Function

Run the **switchport port-security interface mac-address** command to configure static secure addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static secure address is configured by default.

Syntax

switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

no switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

default switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

mac-address *mac-address*: Specifies the static secure address to be configured.

vlan vlan-*id*: Specifies the VLAN to which a MAC address belongs. The value range is from 1 to 4094. This parameter takes effect only for trunk ports.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the static secure address to 00d0.f800.5555 and VLAN ID to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# switchport port-security interface gigabitethernet 0/1 mac-address
00d0.f800.5555 vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 switchport port-security maximum

Function

Run the **switchport port-security maximum** command to configure the maximum number of secure addresses for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default maximum number of secure addresses for a port is **128**.

Syntax

switchport port-security maximum *number*

no switchport port-security maximum

default switchport port-security maximum

Parameter Description

maximum *number*: Specifies the maximum number of secure addresses. The value range is from 1 to 128.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If you set the maximum number of secure addresses for a port to **1** and configure a secure address for this port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port.

The number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. The default value is **128**. If the configured maximum number of secure addresses is smaller than the current number of secure addresses, the configuration fails.

The maximum number of secure addresses takes effect only to secure addresses and is invalid to security bindings.

Caution

If 802.1x is enabled on a port but the number of authenticated users exceeds the maximum number of users configured for port security, port security cannot be enabled.

Examples

The following example sets the maximum number of secure addresses to 2 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security maximum 2
```

Notifications

When the configured maximum number of secure addresses is smaller than the current number of secure addresses, the following notification will be displayed:

```
Setting value is less than the current maximum.
```

Common Errors

The configured maximum number of addresses is smaller than the current number of addresses.

Platform Description

N/A

Related Commands

N/A

1.9 switchport port-security mac-address sticky

Function

Run the **switchport port-security mac-address sticky** command to enable sticky MAC address learning and configure sticky MAC addresses.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Sticky MAC address learning is disabled by default.

Syntax

switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

no switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

default switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

Parameter Description

mac-address: MAC address.

vlan *vlan-id*: Specifies the VLAN to which a MAC address belongs. This parameter takes effect only for trunk ports.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Sticky MAC address learning is used to save MAC addresses dynamically learned by the device to sticky MAC addresses. Sticky MAC addresses are special MAC addresses not affected by the aging mechanism. No matter whether dynamic or static aging is configured, sticky MAC addresses will not be aged.

Examples

The following example configures sticky MAC address 00d0.f800.5555 and VLAN ID 1 for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address sticky
00d0.f800.5555 vlan 1
```

The following example enables sticky MAC address learning for GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security mac-address sticky
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 switchport port-security violation

Function

Run the **switchport port-security violation** command to configure the method for handling packets that violate the port security requirements.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Packets that do not match the security address are discarded by default.

Syntax

switchport port-security violation { **protect** | **restrict** | **shutdown** }

no switchport port-security violation

default switchport port-security violation

Parameter Description

protect: Discards packets that do not match the security address.

restrict: Discards packets that do not match the security address and sends a trap notification.

shutdown: Discards packets that do not match the security address and disables the port.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered. If the violation handling mode of the port is changed after a violation, the new violation handling mode takes effect only after the secure port is restored to the non-violation state and violates the security again.

You can configure the maximum number of secure addresses for a port. If you set the maximum number of secure addresses to **1** for a port and configure a secure address for the port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port.

Examples

The following example enables port security on Gigabitethernet 0/1 and sets the port security violation handling mode to **shutdown**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security
Hostname(config-if-GigabitEthernet 0/1)# switchport port-security violation shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show port-security

Function

Run the **show port-security** command to display port security configurations and secure addresses.

Syntax

show port-security [**all** | [**address** | **binding**] [**interface** *interface-type interface-number*]]

Parameter Description

address: Specifies the secure address to be displayed.

binding: Specifies the security binding to be displayed.

interface *interface-type interface-number*: Specifies the interface whose port security configurations are displayed.

all: Displays all effective secure addresses and security bindings.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified when this command is run (**show port-security**), port security configurations, violation handling, and other information of all interfaces are displayed.

Examples

The following example displays all port security configurations.

```
Hostname> enable
Hostname# show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction AgingTime
                (Count)     (Count)     (Count)        (Count)
(min)
1    Gi0/1     128         2         2           1              protect
Total secure addresses in System : 2
Total secure bindings  in System : 3
```

Table 1-1 Output Fields of the show port-security Command

Field	Description
NO.	Record number
Secure Port	Device port name
MaxSecureAddr(count)	Maximum number of secure addresses allowed on a port
CurrentAddr(count)	Current number of secure addresses on a port
CurrentIpBind (count)	Number of secure IP address bindings on a port
CurrentIpMacBind (count)	Number of secure IP-MAC address bindings on a port
Security Action	Violation handling mode on a port
Total secure addresses in System	Total number of secure addresses configured on a device
Total secure bindings in System	Number of security bindings configured on a device

The following example displays all secure addresses.

```
Hostname> enable
Hostname# show port-security address
NO.  VLAN  MacAddress     PORT                  TYPE      RemainingAge(mins)
STATUS
1    1    00d0.f800.073c  GigabitEthernet 0/1      Configured        --
active
2    1    00d0.f800.073d  GigabitEthernet 0/1      Configured        --
active
```

Table 1-2 Output Fields of the show port-security address Command

Field	Description
NO.	Record number
Vlan	VLAN ID
Mac Address	MAC address
Port	Port name
Type	Method for generating the secure address
Remaining Age(mins)	Address aging time
STATUS	Secure address effective status

The following example displays all security bindings.

```
Hostname> enable
Hostname# show port-security binding
NO.  VLAN MacAddress    PORT      IpAddress                              FilterType
FilterStatus
1    1    00d0.f800.073c Gi0/1     192.168.12.202                          ipv4-mac
active
2    --       --      Gi0/1     192.168.0.1                           ipv4-only
active
3    --       --      Gi0/1     ffaa:ddcc::1                          ipv6-only
active
```

Table 1-3 Output Fields of the show port-security binding Command

Field	Description
NO.	Record number
Vlan	VLAN ID
Mac Address	MAC address
Port	Port name
IpAddress	IP address
FilterType	Security binding filtering type
FilterStatus	Security binding effective status

The following example displays port security configurations of Gigabitethernet 0/1.

```
Hostname> enable
Hostname# show port-security interface gigabitethernet 0/1
```

```
Interface                : GigabitEthernet 0/1
Port status              : down
Port Security            : enabled
SecureStatic address aging   : disabled
Sticky dynamic address      : disabled
Violation mode           : protect
Maximum MAC Addresses       : 128
Total MAC Addresses         : 2
Configured MAC Addresses    : 2
Dynamic MAC Addresses       : 0
Sticky MAC Addresses        : 0
Total security binding      : 3
IPv4-ONLY Binding Addresses  : 1
IPv6-ONLY Binding Addresses  : 1
IPv4-MAC Binding Addresses   : 1
IPv6-MAC Binding Addresses   : 0
Aging time(min)           : 0
```

Table 1-4 Output Fields of the show port-security interface Command

Field	Description
Interface	Device port name
Port status	Device port status
Port Security	Port security enabling status on the port
SecureStatic address aging	Whether secure addresses statically configured on the port will be aged
Sticky dynamic address	Whether secure addresses dynamically learned on the port will be converted to sticky addresses
Violation mode	Violation handling mode on the port
Maximum MAC Addresses	Maximum number of secure addresses allowed on a port
Total MAC Addresses	Number of effective secure addresses
Configured MAC Addresses	Number of statically configured secure addresses
Dynamic MAC Addresses	Number of dynamically configured secure addresses
Sticky MAC Addresses	Number of sticky secure addresses
Total security binding	Number of effective security bindings
IPv4-ONLY Binding Addresses	Number of security bindings with only IPv4 addresses

Field	Description
IPv6-ONLY Binding Addresses	Number of security bindings with only IPv6 addresses
IPv4-MAC Binding Addresses	Number of security bindings with IPv4 and MAC addresses
IPv6-MAC Binding Addresses	Number of security bindings with IPv6 and MAC addresses
Aging time(min)	Secure address aging time

Notifications

N/A

Platform Description

N/A

1 IP Source Guard Commands

Command	Function
ip source binding	Add static user information to the source IP address binding database.
ip source binding sticky-mac	Enable the function of converting source IP address binding entries to static MAC address entries.
ip verify source	Enable IP Source Guard on an interface or a VLAN.
ip verify source dai-source	Enable the sole role of the source IP address binding database as the source of Dynamic ARP Inspection (DAI) binding entries.
ip verify source exclude-vlan	Specify an excluded VLAN for IP Source Guard on an interface.
ip verify source trust	Configure an IP Source Guard trusted interface.
show ip source binding	Display information of the source IP address binding database.
show ip source binding sticky-mac	Display information about source IP address binding entries converted to static MAC address entries.
show ip verify source	Display user filtering entries of IP Source Guard.

1.1 ip source binding

Function

Run the **ip source binding** command to add static user information to the source IP address binding database.

Run the **no** form of this command to remove this configuration.

No static user information is added by default.

Syntax

ip source binding *mac-address* **vlan** *vlan-id ipv4-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

no ip source binding *mac-address* **vlan** *vlan-id ipv4-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

Parameter Description

mac-address: Media access control (MAC) address of a statically added user.

vlan-id: ID of the virtual local area network (VLAN) to which a statically added user belongs. For products that support QinQ termination, it refers to the outer VLAN ID of a user.

ipv4-address: IPv4 address of a statically added user.

interface *interface-type interface-number*: Specifies the interface statically added.

ip-mac: Specifies that the IP address and MAC address binding type is used globally.

ip-only: Specifies that the IP address binding type is used globally.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by Dynamic Host Configuration Protocol (DHCP).

This command can be configured only on L2 switching interfaces, L2 aggregation ports (link aggregation), and encapsulation subinterfaces. When this command is configured on other types of interfaces, the configuration will fail.

Users can configure global binding user records to enable legitimate users to pass IP Source Guard detection on all interfaces.

Note

- A configured binding record takes effect either on the access interface or globally.
- When duplicate user records exist, attributes of the new record will overwrite those of the old record.

Examples

The following example adds a static user record to the source IP address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IP address is 1.1.1.1, and the interface is GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
gigabitethernet 0/1
```

The following example adds a static user record to the source IP address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IP address is 1.1.1.1, and the filtering type is IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
```

Notifications

When the **no** form of this command is run to delete static configuration and the entered parameters are different from those previously configured, the following notification will be displayed:

```
% Failed to execute command, because of "No such binding entry [mac 0000.0000.0001 ip
1.1.1.1 vlan 2  GLOBAL]".
```

When a user record is configured and the entered wired interface is not an L2 switching interface, L2 aggregation port, or encapsulation sub-interface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current
interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip source binding sticky-mac

Function

Run the **ip source binding sticky-mac** command to enable the function of converting source IP address binding entries to static MAC address entries.

Run the **no** form of this command to disable this feature.

The function of converting source IP address binding entries to static MAC address entries is disabled by default.

Syntax

ip source binding sticky-mac

no ip source binding sticky-mac

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The MAC address table records mapping between MAC addresses and interfaces. Unauthorized users can use MAC addresses of legitimate users to refresh MAC address table records, which will cause abnormal packet forwarding in the network. To prevent unauthorized users from refreshing the MAC address table to launch network attacks, configure this command in interface configuration mode to convert source IP address binding entries to static MAC address entries.

Examples

The following example enables the function of converting source IP address binding entries to static MAC address entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip source binding sticky-mac
```

Notifications

When the function of converting source IP address binding entries to static MAC address entries is enabled after the DHCP Snooping binding entry migration function is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When the function of converting source IP address binding entries to static MAC address entries is enabled on an interface after an access security control option, such as web authentication, 802.1x authentication, or port security is enabled on the interface, the following notification will be displayed:

```
%IP_SRC_GRD-STICKY_MAC: Failed to open sticky mac on interface [Interface name].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip verify source

Function

Run the **ip verify source** command to enable IP Source Guard on an interface or a VLAN.

Run the **no** form of this command to disable this feature.

IP Source Guard is disabled on an interface or a VLAN by default.

Syntax

ip verify source [**port-security**]

no ip verify source

Parameter Description

port-security: Configures IP Source Guard based on IP address and MAC address.

Command Modes

Interface configuration mode

VLAN configuration mode

Default Level

14

Usage Guidelines

After IP Source Guard is enabled for an interface or a VLAN, users can detect IP packets passing through the interface or VLAN based on the IP address or IP address and MAC address.

This command can be configured only on L2 switching interfaces, L2 aggregation ports, encapsulation subinterfaces, and VLAN configuration mode. When this command is configured on other types of interfaces, the configuration will fail.

When IP Source Guard is enabled in VLAN configuration mode, it is effective to all L2 interfaces in the VLAN. Users need to configure the **ip verify source trust** command on the uplink interface to specify trusted interfaces. Otherwise, packet forwarding may fail.

Caution

Legitimate users of IP Source Guard come from DHCP Snooping and static user configuration. If IP Source Guard is enabled on an interface but no valid data source is configured, users who access the network through the interface cannot use the network normally.

Examples

The following example enables IP Source Guard on GigabitEthernet 0/1 and detects packets only based on the IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
```

The following example enables IP Source Guard on GigabitEthernet 0/1 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source port-security
```

The following example enables IP Source Guard on VLAN 1 and detects packets only based on the IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source
```

The following example enables IP Source Guard on VLAN 1 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source port-security
```

Notifications

When this command is configured on a DHCP trusted interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in interface name".
```

Common Errors

- IP Source Guard is enabled. However, the source of legitimate user records is not configured.

Platform Description

N/A

Related Commands

N/A

1.4 ip verify source dai-source

Function

Run the **ip verify source dai-source** command to enable the sole role of the source IP address binding database as the source of Dynamic ARP Inspection (DAI) binding entries.

Run the **no** form of this command to remove this configuration.

The sole role of the source IP address binding database as the source of DAI binding entries is not configured by default.

Syntax

ip verify source dai-source

no ip verify source dai-source

Parameter Description

N/A

Command Modes

Interface configuration mode

VLAN configuration mode

Default Level

14

Usage Guidelines

After the sole role of the source IP address binding database as the source of DAI binding entries is configured, the bound entries are solely used for DAI and are not assigned to hardware.

This command can be configured either in interface configuration mode or VLAN configuration mode.

Examples

The following example enables the sole role of the source IP address binding database as the source of DAI binding entries on switching interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source dai-source
```

The following example enables the sole role of the source IP address binding database as the source of DAI binding entries on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source dai-source
```

Notifications

When this command is configured on a DHCP Snooping or IP Source Guard trusted interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in interface name".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip verify source exclude-vlan

Function

Run the **ip verify source exclude-vlan** command to specify an excluded VLAN for IP Source Guard on an interface.

Run the **no** form of this command to remove this configuration.

The function of specifying excluded VLANs for IP Source Guard on an interface is disabled by default.

Syntax

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

vlan-id: ID of the VLAN that is not controlled by IP Source Guard on an interface. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By using this command, the specified VLANs under an interface where the IP Source Guard function is enabled can be exempted from check and filtering.

After IP Source Guard is disabled on the interface, the specified excluded VLANs will be cleared automatically.

This command can be configured on L2 switching interfaces or encapsulation subinterfaces.

Caution

An excluded VLAN can be specified for an interface only after IP Source Guard is enabled on the interface.

Examples

The following example specifies VLAN 1 as an excluded VLAN for IP Source Guard on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
Hostname(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip verify source trust

Function

Run the **ip verify source trust** command to configure an IP Source Guard trusted interface.

Run the **no** form of this command to remove this configuration.

No IP Source Guard trusted interface is configured by default.

Syntax

ip verify source trust

no ip verify source trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The IP Source Guard trusted interface function is mutually exclusive with the IP Source Guard interface, port security, 802.1x authorization, and Address Resolution Protocol (ARP) check services.

When an interface is configured as an IP Source Guard trusted interface, IP Source Guard is not performed for the interface and packets through this interface are released directly.

This command can be configured on L2 switching interfaces and L2 aggregation ports (link aggregation).

Caution

This command is used only to enable IPv6 Source Guard for a VLAN.

Examples

The following example configures GigabitEthernet 0/1 as an IP Source Guard trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source trust
```

Notifications

When this command is configured on an IPv6 Source Guard security interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict ".
```

Common Errors

- An IP Source Guard security interface is configured as an IP Source Guard trusted interface.

Platform Description

N/A

Related Commands

N/A

1.7 show ip source binding

Function

Run the **show ip source binding** command to display information of the source IP address binding database.

Syntax

show ip source binding [*ipv4-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]

Parameter Description

Ipv4-address: IPv4 address whose user binding information is displayed.

mac-address: MAC address whose user binding information is displayed.

vlan-id: VLAN whose user binding information is displayed.

interface-type interface-number: Wired access interface whose user binding information is displayed.

dhcp-snooping: Displays binding information of a dynamic user.

static: Displays binding information of a static user.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of the source IP address binding database.

```
Hostname> enable
Hostname# show ip source binding static
NO.   MACADDRESS        IPADDRESS      LEASE(SEC)   TYPE         VLAN  INTERFACE
1     0001.0002.0001    1.2.3.2        Infinite     Static       1     Global
2     0001.0002.0002    1.2.3.3        Infinite     Static       1
GigabitEthernet 0/1
3     0001.0002.0003    1.2.3.4        Infinite     Static       1     Global
4     0001.0002.0004    1.2.3.5        Infinite     Static       1     Global
Total number of bindings: 4
```

Table 1-1 Output Fields of the show ip source binding Command

Field	Description
Total number of bindings	Number of bindings in the binding database
NO.	Record number
MACADDRESS	MAC address of a user
IPADDRESS	IP address of a user
LEASE(SEC)	Lease time of a record
TYPE	Record type
VLAN	VLAN to which a user belongs
INTERFACE	Interface name

Notifications

N/A

Platform Description

N/A

Related Commands

- **ip source binding**

1.8 show ip source binding sticky-mac

Function

Run the **show ip source binding sticky-mac** command to display information about source IP address binding entries converted to static MAC address entries.

Syntax

show ip source binding sticky-mac [**interface** *interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface under which information about source IP address binding entries converted to static MAC address entries is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about source IP address binding entries converted to static MAC address entries.

```
Hostname> enable
Hostname# show ip source binding sticky-mac
Total number of bindings: 2
NO.   MACADDRESS        TYPE         VLAN  INTERFACE
1     2018.0012.0017    Static       1     GigabitEthernet 0/1
2     2018.0012.0018    DHCP-Snooping 1     GigabitEthernet 0/1
```

Table 1-2 Output Fields of the show ip source binding sticky-mac Command

Field	Description
Total number of bindings	Number of source IP address binding entries converted to static MAC address entries
NO	Record number
MACADDRESS	MAC address of a user
TYPE	Record type of a binding entry
VLAN	VLAN to which a user belongs
INTERFACE	User access interface

Notifications

N/A

Platform Description

N/A

Related Commands

- ip source binding sticky-mac

1.9 show ip verify source

Function

Run the **show ip verify source** command to display user filtering entries of IP Source Guard.

Syntax

show ip verify source [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface-type interface-number: Interface whose user filtering entries are displayed.

vlan *vlan-id*: Specifies the VLAN whose user filtering entries are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays user filtering entries of IP Source Guard.

```
Hostname> enable
Hostname# show ip verify source
NO.   INTERFACE          FilterType  FilterStatus         IPADDRESS
MACADDRESS     VLAN TYPE
1     Global             IP+MAC     Inactive-not-apply    192.168.0.127
0001.0002.0003  1 Static
2     Global             IP-ONLY    Active              1.2.3.7
0001.0002.0007  1 Static
3     Global             IP+MAC     Active              1.2.3.6
0001.0002.0006  1 Static
4     GigabitEthernet 0/1  UNSET      Inactive-restrict-off  1.2.3.9
0001.0002.0009  1 DHCP-Snooping
5     GigabitEthernet 0/5  IP-ONLY    Active              Deny-All
```

Table 1-3 Output Fields of the show ip verify source Command

Field	Description
Total number of bindings	Number of assigned bindings

Field	Description
NO.	Record number
INTERFACE	User access interface
FilterType	Record type of a binding entry
FilterStatus	Record status of a binding entry ● **Inactive-restrict-off**: IP Source Guard is disabled for the interface to which a binding record belongs. ● **Inactive-not-apply**: A bound user record cannot be converted to a filtering entry due to system errors. ● **Active**: The filtering entry corresponding to the bound user record has taken effect.
IPADDRESS	IP address of a user
MACADDRESS	MAC address of a user
VLAN TYPE	VLAN to which a user belongs

Notifications

N/A

Platform Description

N/A

Related Commands

- **ip verify source**

1 IPv6 Source Guard Commands

Command	Function
ipv6 source binding	Add static user information to the IPv6 source address binding database.
ipv6 source binding sticky-mac	Enable the function of converting IPv6 source address binding entries to static MAC address entries.
ipv6 verify source	Enable IPv6 Source Guard on an interface or a VLAN.
ipv6 verify source permit link-local	Enable local link address release on an interface.
ipv6 verify source trust	Configure an interface as an IPv6 Source Guard trusted interface.
show ipv6 source binding	Display information of the IPv6 source address binding database.
show ipv6 source binding sticky-mac	Display information about IPv6 source address binding entries converted to static MAC address entries.

1.1 ipv6 source binding

Function

Run the **ipv6 source binding** command to add static user information to the IPv6 source address binding database.

Run the **no** form of this command to remove this configuration.

No static user information is added by default.

Syntax

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

no ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

Parameter Description

mac-address: Media access control (MAC) address of a statically added user.

vlan-id: ID of the virtual local area network (VLAN) to which a statically added user belongs.

ipv6-address: IPv6 address of a statically added user.

interface *interface-type interface-number*: Specifies the interface to which a statically added user belongs.

ip-mac: Specifies that the IPv6 address and MAC address binding type is used globally.

ip-only: Specifies that the IPv6 address binding type is used globally.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Through this command, legitimate users can pass IPv6 Source Guard detection instead of being controlled by Dynamic Host Configuration Protocol version 6 (DHCPv6).

This command can be configured only on L2 switching interfaces and L2 aggregation ports (link aggregation). When this command is configured on other types of interfaces, the configuration will fail.

Users can configure global binding user records to enable legitimate users to pass IPv6 Source Guard detection on all interfaces.

A configured binding record takes effect either on the access interface, VLAN, or globally.

When duplicate user records exist, attributes of the new record will overwrite those of the old record.

Examples

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the interface is GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 interface
gigabitethernet 0/1
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-mac
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address that takes effect globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-only
```

Notifications

When the **no** form of this command is run to delete static configuration and the entered parameters are different from those previously configured, the following notification will be displayed:

```
% Failed to execute command, because of "No such binding entry".
```

When a user record is configured and the entered access interface is not an L2 switching interface or L2 aggregation port, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current
interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ipv6 source binding sticky-mac

Function

Run the **ipv6 source binding sticky-mac** command to enable the function of converting IPv6 source address binding entries to static MAC address entries.

Run the **no** form of this command to disable this feature.

The function of converting IPv6 source address binding entries to static MAC address entries is disabled by default.

Syntax

ipv6 source binding sticky-mac

no ipv6 source binding sticky-mac

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The MAC address table records mapping between MAC addresses and interfaces. Unauthorized users can use MAC addresses of legitimate users to refresh MAC address table records, which will cause abnormal packet forwarding in the network. To prevent unauthorized users from refreshing the MAC address table to launch network attacks, configure this command in interface configuration mode to convert IPv6 source address binding entries to static MAC address entries.

Examples

The following example enables the function of converting IPv6 source address binding entries to static MAC address entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 source binding sticky-mac
```

Notifications

When the function of converting IPv6 source address binding entries to static MAC address entries is enabled on an interface after an access security control option, such as web authentication, 802.1x authentication, or port security, is enabled on the interface, the following notification will be displayed:

```
Failed to open sticky mac on interface [Interface name].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ipv6 verify source

Function

Run the **ipv6 verify source** command to enable IPv6 Source Guard on an interface or a VLAN.

Run the **no** form of this command to disable this feature.

IPv6 Source Guard is disabled on an interface or a VLAN by default.

Syntax

ipv6 verify source [**port-security**]

no ipv6 verify source

Parameter Description

port-security: Configures IPv6 Source Guard based on IPv6 address and MAC address.

Command Modes

VLAN configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

By enabling IPv6 Source Guard on an interface or a VLAN through this command, users can detect packets based on the IPv6 address or IPv6 address and MAC address.

This command can be configured only on L2 switching interfaces and L2 aggregation ports in interface configuration mode. When this command is configured on other types of interfaces, the configuration will fail.

Caution

Legitimate users of IPv6 Source Guard come from DHCPv6 Snooping/ND Snooping and static user configuration. If IPv6 Source Guard is enabled on an interface but no valid data source is configured, users who access the network through IPv6 cannot use the network normally.

Examples

The following example enables IPv6 Source Guard on GigabitEthernet 0/1 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source
```

The following example enables IPv6 Source Guard on GigabitEthernet 0/1 and detects packets based on the IPv6 address and MAC address.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source port-security
```

The following example enables IPv6 Source Guard on VLAN 1 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ipv6 verify source
```

The following example enables IPv6 Source Guard on VLAN 1 and detects packets based on the IPv6 address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ipv6 verify source port-security
```

The following example enables IP Source Guard on VLANs 2-5 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-5
Hostname(config-vlan-range)# ipv6 verify source
```

The following example enables IP Source Guard on VLANs 2-5 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-5
Hostname(config-vlan-range)# ipv6 verify source port-security
```

Notifications

When this command is configured on a DHCPv6 or an IPv6 Source Guard trusted interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

Common Errors

- IPv6 Source Guard is enabled. However, the source of legitimate user records is not configured.
- IPv6 Source Guard is enabled on a VLAN. However, the uplink interface is not configured as a trusted interface.

Platform Description

N/A

Related Commands

N/A

1.4 ipv6 verify source permit link-local

Function

Run the **ipv6 verify source permit link-local** command to enable local link address release on an interface.

Run the **no** form of this command to disable this feature.

The local link address release function is disabled on an interface by default.

Syntax

ipv6 verify source permit link-local

no ipv6 verify source permit link-local

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the local link address release function is enabled on an interface by running this command, packets with FE80::/10 or ::/128 as source addresses will not be checked.

When ND Snooping is disabled, entry addresses come from only DHCPv6 addresses and do not contain local link addresses. However, some terminals use local link addresses to access the gateway or other addresses in the same network segment. In addition, local link addresses are required for addressing, Duplicate Address Detection (DAD), and other operations before DHCPv6 exchange. Therefore, in DHCPv6 Snooping + IPv6 Source Guard scenarios, run the **ipv6 verify source permit link-local** command to release local link addresses (fe80::/10) and undefined addresses (::/128).

This command can be configured only on L2 switching interfaces and L2 aggregation ports.

Caution

The local link address release function needs to be configured only when both DHCPv6 Snooping and IPv6 Source Guard are enabled and ND Snooping is disabled. The configuration command for the local link address release function is independent of the DHCPv6 Snooping, IPv6 Source Guard, and ND Snooping commands.

Examples

The following example enables local link address release on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source permit link-local
```

Notifications

When this command is configured on an AP member interface, the following notification will be displayed:

```
Configure is not supported on current interface.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 verify source trust

Function

Run the **ipv6 verify source trust** command to configure an interface as an IPv6 Source Guard trusted interface.

Run the **no** form of this command to remove this configuration.

No interface is configured as an IPv6 Source Guard trusted interface by default.

Syntax

ipv6 verify source trust

no ipv6 verify source trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When an interface is configured as an IPv6 Source Guard trusted interface, IPv6 Source Guard is not performed for the interface and packets through this interface are released directly.

This command can be configured on L2 switching interfaces and L2 aggregation ports (link aggregation).

Caution

This command is used only to enable IPv6 Source Guard for a VLAN.

Examples

The following example configures GigabitEthernet 0/1 as an IPv6 Source Guard trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source trust
```

Notifications

When this command is configured on an IPv6 Source Guard security interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict ".
```

Common Errors

- An IPv6 Source Guard security interface is configured as an IPv6 Source Guard trusted interface.

Platform Description

N/A

Related Commands

- **ipv6 verify source**

1.6 show ipv6 source binding

Function

Run the **show ipv6 source binding** command to display information of the IPv6 source address binding database.

Syntax

show ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]

Parameter Description

ipv6-address: IPv6 address whose user binding information is displayed.

mac-address: MAC address whose user binding information is displayed.

vlan *vlan-id*: Specifies the VLAN whose user binding information is displayed.

interface *interface-type interface-number*: Specifies the interface whose user binding information is displayed.

dhcp-snooping: Displays binding information of dynamic users.

static: Displays binding information of static users.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of the IPv6 source address binding database.

```
Hostname> enable
Hostname# show ipv6 source binding
Total entries found: 2
No.    Ipv6 Address                          Mac Address    VLAN Interface Type
1      2017::2                               00e0.4c36.077d 100  GLOBAL
Static/DHCPv6
2      2017::3                               9890.96ca.c3d5 100  GLOBAL    Static
```

Table 1-1 Output Fields of the show ipv6 source binding Command

Field	Description
Total number of bindings	Number of bindings in the binding database
NO	Record number
Ipv6 Address	IPv6 address of a user
Mac Address	MAC address of a user
VLAN	VLAN to which a user belongs
Interface	Interface name or global interface
Type	Record type

Notifications

N/A

Platform Description

N/A

Related Commands

- **ipv6 source binding**

1.7 show ipv6 source binding sticky-mac

Function

Run the **show ipv6 source binding sticky-mac** command to display information about IPv6 source address binding entries converted to static MAC address entries.

Syntax

show ipv6 source binding sticky-mac [**interface** *interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface under which information about IPv6 source address binding entries converted to static MAC address entries is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about IPv6 source address binding entries converted to static MAC address entries.

```
Hostname> enable
Hostname# show ipv6 source binding sticky-mac
Total number of bindings: 1
NO.   MACADDRESS        VLAN  INTERFACE
1     2018.0012.0017     1    GigabitEthernet 0/1
```

Table 1-2 Output Fields of the show ipv6 source binding sticky-mac Command

Field	Description
Total number of bindings	Number of assigned bindings
NO.	Record number
MACADDRESS	MAC address of a user
VLAN	VLAN to which a user belongs
INTERFACE	User access interface

Notifications

N/A

Platform Description

N/A

Related Commands

- **ipv6 source binding sticky-mac**

1 SAVI Commands

Command	Function
savi ipv6 bind-source add	Configure the data sources of Source Address Validation Improvement (SAVI) binding entries.
savi ipv6 check permit link-local	Enable SAVI to permit local link addresses and undefined addresses.
savi ipv6 check source exclude-vlan	Configure excluded virtual local area networks (VLANs) for SAVI on an interface.
savi ipv6 check source ip-address	Enable IPv6 SAVI.
savi ipv6 station-move	Enable binding entry migration.
savi ipv6 source binding vlan	Add static user information to the IPv6 source address binding database.
show savi ipv6 check source	Display effective SAVI filtering entries.
show savi ipv6 source binding	Display binding entries learned by SAVI.

1.1 savi ipv6 bind-source add

Function

Run the **savi ipv6 bind-source add** command to configure the data sources of Source Address Validation Improvement (SAVI) binding entries.

Run the **no** form of this command to remove this configuration.

Binding entries generated during the stateless address autoconfiguration (SLAAC) and Dynamic Host Configuration Protocol version 6 (DHCPv6) processes are used as the sources of dynamic binding entries by default. Binding entries can also be statically configured.

Syntax

savi ipv6 bind-source add { **dhcp** | **slaac** }

no savi ipv6 bind-source add { **dhcp** | **slaac** }

Parameter Description

dhcp: Uses binding entries snooped during the DHCPv6 process as a source of SAVI binding entries.

slaac: Uses binding entries snooped during the SLAAC process as a source of SAVI binding entries.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Neighbor discovery (ND) Snooping is used to snoop the SLAAC process. When entries generated during ND Snooping are configured as a source of SAVI binding entries, ND Snooping needs to be enabled.

DHCPv6 Snooping is used to snoop the DHCPv6 process. When entries generated during DHCPv6 Snooping are configured as a source of SAVI binding entries, DHCPv6 Snooping needs to be enabled.

Examples

The following example cancels entries generated during SLAAC as a source of SAVI binding entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no savi ipv6 bind-source add slaac
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 savi ipv6 check permit link-local

Function

Run the **savi ipv6 check permit link-local** command to enable SAVI to permit local link addresses and undefined addresses.

Run the **no** form of this command to remove this configuration.

Permitting local link addresses and undefined addresses is not configured by default.

Syntax

savi ipv6 check permit link-local

no savi ipv6 check permit link-local

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After SAVI is enabled on an interface, SAVI checks the validity of source IPv6 addresses in IPv6 packets transmitted through the interface. After configuring this command, SAVI permits all IPv6 packets with fe80::/10 and ::/128 as source addresses.

Caution

Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

Examples

The following example enables SAVI to permit local link addresses and undefined addresses.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# savi ipv6 check permit link-local
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 savi ipv6 check source exclude-vlan

Function

Run the **savi ipv6 check source exclude-vlan** command to configure excluded virtual local area networks (VLANs) for SAVI on an interface.

Run the **no** form of this command to remove this configuration.

No excluded VLANs for SAVI are configured on an interface by default.

Syntax

savi ipv6 check source exclude-vlan *vlan-id*

no savi ipv6 check source exclude-vlan *vlan-id*

Parameter Description

vlan-id: VLAN for which SAVI is not performed. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After SAVI is enabled, you can run this command to permit IPv6 packets from specified VLANs.

After SAVI is disabled, the specified excluded VLANs are deleted.

Examples

The following example configures excluded VLANs for SAVI on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# savi ipv6 check source ip-address
mac-address
Hostname(config-if-GigabitEthernet 0/1)# savi ipv6 check source exclude-vlan 1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.4 savi ipv6 check source ip-address

Function

Run the **savi ipv6 check source ip-address** command to enable IPv6 SAVI.

Run the **no** form of this command to disable this feature.

IPv6 SAVI is disabled by default.

Syntax

savi ipv6 check source ip-address [**mac-address**]

no savi ipv6 check source

Parameter Description

mac-address: Enables media access control (MAC) address check at the same time. The filtering mode is set to IP address and MAC address.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can run this command on a DHCPv6 Snooping/ND Snooping untrusted interface to check the validity of source IPv6 addresses in IPv6 packets through the interface. If the filtering mode is set to IP address and MAC address, the validity of the source MAC address in the Ethernet header will also be checked.

Examples

The following example sets the filtering mode of IPv6 SAVI to IP address and MAC address on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# savi ipv6 check source ip-address
mac-address
```

Notifications

When a security mode conflict occurs, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

Platform Description

N/A

Related Commands

N/A

1.5 savi ipv6 station-move

Function

Run the **savi ipv6 station-move** command to enable binding entry migration.

Run the **no** form of this command to disable this feature.

The binding entry migration function is disabled by default.

Syntax

savi ipv6 station-move

no savi ipv6 **station-move**

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the binding entry migration function is enabled, dynamic binding entries can be migrated to the corresponding VLANs and interfaces automatically based on changes of the MAC address table. In wireless scenarios, when a host does not re-obtain an IPv6 address after it roams, the access point (AP) after roaming does not match the SAVI binding entry. As a result, the host cannot access the network. When the binding entry migration function is enabled, SAVI can perceive host migration based on MAC address table changes and update SAVI binding entries.

SAVI binding entry migration is triggered by DHCPv6/ND Snooping binding entry migration.

Caution

After binding entry migration is enabled, security functions are weakened and forged MAC address communication by attackers cannot be prevented.

Examples

The following example enables binding entry migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# savi ipv6 station-move
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 savi ipv6 source binding vlan

Function

Run the **savi ipv6 source binding vlan** command to add static user information to the IPv6 source address binding database.

Run the **no** form of this command to remove this configuration.

No static user information is added by default.

Syntax

savi ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

no savi ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

Parameter Description

mac-address: MAC address of a statically added user.

vlan-id: ID of the VLAN to which a statically added user belongs.

ipv6-address: IPv6 address of a statically added user.

interface-type interface-number: Type and number of the interface to which a statically added user belongs.

ip-mac: Specifies the IPv6 address and MAC address binding type.

ip-only: Specifies the IPv6 address binding type.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to permit packets from a specified user.

This command can be configured only on L2 switching interfaces, L2 aggregation ports (link aggregation), and encapsulation subinterfaces. When this command is configured on other types of interfaces, the configuration will fail.

Note

- A configured binding record takes effect either on the access interface or globally.
- When duplicate user records exist, attributes of the new record will overwrite those of the old record.

Examples

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the interface is GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# savi ipv6 source binding 0000.0000.0001 vlan 1 1::1 interface
gigabitethernet 0/1
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# savi ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-mac
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# savi ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-only
```

Notifications

When the **no** form of this command is run to delete static configuration and the entered parameters are different from those previously configured, the following notification will be displayed:

```
% Failed to execute command, because of "No such binding entry".
```

When a user record is configured and the entered wired access interface is not an L2 switching interface, L2 aggregation port, or encapsulation subinterface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface"
```

Platform Description

N/A

Related Commands

N/A

1.7 show savi ipv6 check source

Function

Run the **show savi ipv6 check source** command to display effective SAVI filtering entries.

Syntax

show savi ipv6 check source [*ipv6-address* | **interface** *interface-type interface-number*]

Parameter Description

ipv6-address: IPv6 address whose filtering information is displayed.

interface-type interface-number: Interface whose effective binding entries are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays effective SAVI filtering entries.

```
Hostname> enable
Hostname# show savi ipv6 check source
Total entries found: 6
No.    Ipv6 Address                        Mac Address    VLAN Interface Filter
0      2018:2::1                           8005.8820.182b 2    Gi0/1     IP+MAC
1      2018:3::1                           8005.8820.182b 3    Gi0/1     IP+MAC
2      2018:4::1                           8005.8820.182b 4    Gi0/1     IP+MAC
3      fe80::8205:88ff:fe20:182b              8005.8820.182b 2    Gi0/1     IP+MAC
```

Table 1-1 Output Fields of the show savi ipv6 check source Command

Field	Description
Total entries found	Number of effective bindings
NO	Record number
IPv6 Address	IPv6 address of a user
MacAddress	MAC address of a user
VLAN	VLAN to which a user belongs
Interface	Interface name

Notifications

N/A

Platform Description

N/A

Related Commands

- **savi ipv6 check source ip-address**

1.8 show savi ipv6 source binding

Function

Run the **show savi ipv6 source binding** command to display binding entries learned by SAVI.

Syntax

show savi ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**type** { **dhcp** | **slaac** | **static** }]

Parameter Description

ipv6-address: IPv6 address whose binding entries are displayed.

mac-address: MAC address whose binding entries are displayed.

vlan *vlan-id*: Specifies the VLAN whose binding entries are displayed.

interface *interface-type interface-number*: Specifies the interface whose binding entries are displayed.

dhcp: Displays binding entries from the DHCPv6 process.

slaac: Displays binding entries from the SLAAC process.

static: Displays statically configured binding entries.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays SAVI-learned binding entries.

```
Hostname> enable
Hostname# show savi ipv6 source binding
Total entries found: 6
No.    Ipv6 Address                          Mac Address    VLAN Interface Type
0      2018:2::1                             8005.8820.182b 2    Gi0/1     SLAAC
1      2018:3::1                             8005.8820.182b 3    Gi0/1     SLAAC
2      2018:4::1                             8005.8820.182b 4    Gi0/1     SLAAC
3      fe80::8205:88ff:fe20:182b               8005.8820.182b 2    Gi0/1     SLAAC
```

Table 1-2 Output Fields of the show savi ipv6 source binding Command

Field	Description
Total entries found	Number of binding entries
NO.	Record number

Field	Description
IPv6 Address	IPv6 address of a user
Mac Address	MAC address of a user
VLAN	VLAN to which a user belongs
Interface	Interface name
Type	Record type

Notifications

N/A

Platform Description

N/A

Related Commands

- **savi ipv6 source binding**

1 ARP Check Commands

Command	Function
arp-check	Enable Address Resolution Protocol (ARP) Check.
show interfaces arp-check list	Display effective ARP Check entries on an interface.

1.1 arp-check

Function

Run the **arp-check** command to enable Address Resolution Protocol (ARP) Check.

Run the **no** form of this command to disable this feature.

ARP Check is disabled by default.

Syntax

arp-check

no arp-check

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Legitimate user information generated by security application modules is used to filter out invalid ARP packets in networks.

Examples

The following example enables ARP Check on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 show interfaces arp-check list

Function

Run the **show interfaces arp-check list** command to display effective ARP Check entries on an interface.

Syntax

show interfaces [*interface-type interface-number*] **arp-check list**

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays effective ARP Check entries on an interface.

```
Hostname> enable
Hostname(config)# show interfaces arp-check list
INTERFACE               SENDER MAC      SENDER IP       POLICY SOURCE
GigabitEthernet 0/1       00D0.F800.0003   192.168.1.3     address-bind
GigabitEthernet 0/1       00D0.F800.0001   192.168.1.1     port-security
GigabitEthernet 0/4                      192.168.1.3     port-security
GigabitEthernet 0/5       00D0.F800.0003   192.168.1.3     address-bind
GigabitEthernet 0/7       00D0.F800.0006   192.168.1.6     AAA ip-auth-mode
GigabitEthernet 0/8       00D0.F800.0007   192.168.1.7     GSN
```

Table 1-1 Output Fields of the show interfaces arp-check list Command

Field	Description
INTERFACE	Interface name
SENDER MAC	Source MAC address
SENDER IP	Source IP address
POLICY SOURCE	Record source

Notifications

N/A

Platform Description

N/A

Related Commands

- **arp-check**

1 DAI Commands

Command	Function
ip arp inspection trust	Configure an L2 interface as a Dynamic APR Inspection (DAI) trusted interface.
ip arp inspection validate interface	Enable DAI to check interface information.
ip arp inspection vlan	Enable DAI on a VLAN.
show ip arp inspection vlan	Display the DAI status on a VLAN.
show ip arp inspection interface	Display the DAI trust status of an interface.

1.1 ip arp inspection trust

Function

Run the **ip arp inspection trust** command to configure an L2 interface as a Dynamic APR Inspection (DAI) trusted interface.

Run the **no** form of this command to remove this configuration.

L2 interfaces are DAI untrusted interfaces by default.

Syntax

ip arp inspection trust

no ip arp inspection trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To enable Address Resolution Protocol (ARP) packets received through an interface to pass DAI unconditionally, set the interface as a DAI trusted interface.

Examples

The following example configures GigabitEthernet 0/1 as a DAI trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip arp inspection trust
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip arp inspection validate interface

Function

Run the **ip arp inspection validate interface** command to enable DAI to check interface information.

Run the **no** form of this command to remove the configuration.

After DAI is enabled, interface information will be checked by default.

Syntax

ip arp inspection validate interface

no ip arp inspection validate interface

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command has been replaced by the **ip dhcp snooping station-move permit** command and is not recommended. Binding entry re-generation is supported in one virtual local area network (VLAN) and is not supported in sub VLANs.

Examples

The following example cancels interface information check by DAI.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip arp inspection validate interface
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip dhcp snooping station-move permit (IP Services/DHCP Snooping Commands)**

1.3 ip arp inspection vlan

Function

Run the **ip arp inspection vlan** command to enable DAI on a VLAN.

Run the **no** form of this command to disable this feature.

DAI is disabled on all VLANs by default.

Syntax

ip arp inspection vlan { *vlan-min* [*vlan-max*] | *vlan-range* }

no ip arp inspection vlan { *vlan- min* [*vlan-max*] | *vlan-range* }

Parameter Description

vlan-min: VLAN ID or the minimum value of a VLAN range for which DAI is performed. The value range is from 1 to 4094.

vlan-max: Maximum value of a VLAN range for which DAI is performed. The value range is from 1 to 4094.

vlan-range: VLAN range for which DAI is enabled. For example, 1, 3–5, 7, and 9–11.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To enable this command to take effect, enable ARP Check first.

Caution

Not all interfaces on a VLAN can be enabled with ARP Check. When an interface is a Dynamic Host Configuration Protocol (DHCP) Snooping trusted interface, no security check rule can be configured on the interface.

Examples

The following example enables DAI on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip arp inspection
Hostname(config)# ip arp inspection vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show ip arp inspection vlan

Function

Run the **show ip arp inspection vlan** command to display the DAI status on a VLAN.

Syntax

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

Parameter Description

vlan-id: VLAN whose DAI status is displayed. The value range is from 1 to 4094.

vlan-range: VLAN range whose DAI status is displayed, for example, 1, 3–5, 7, and 9–11.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the DAI status on all VLANs.

```
Hostname> enable
Hostname# show ip arp inspection vlan
Vlan    Configuration
1       Enable
3       Enable
```

Table 1-1 Output Fields of the show ip arp inspection vlan Command

Field	Description
Vlan	VLAN ID
Configuration	DAI enabling status

Notifications

N/A

Platform Description

N/A

Related Commands

- ip arp inspection vlan

1.5 show ip arp inspection interface

Function

Run the **show ip arp inspection interface** command to display the DAI trust status of an interface.

Syntax

show ip arp inspection interface

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the DAI trust status of all interfaces.

```
Hostname> enable
Hostname# show ip arp inspection interface
Interface              Trust State
GigabitEthernet 0/1      Trusted
Default                Untrusted
```

Table 1-2 Output Fields of the show ip arp inspection interface Command

Field	Description
Interface	Interface name
Trust State	Trust status

Notifications

N/A

Platform Description

N/A

Related Commands

- **ip arp inspection trust**

1 ARP Spoofing Prevention Commands

Command	Function
anti-arp-spoofing ip	Enable gateway-targeted Address Resolution Protocol (ARP) spoofing prevention.
show anti-arp-spoofing	Display data on gateway-targeted ARP spoofing prevention on all interfaces.

1.1 anti-arp-spoofing ip

Function

Run the **anti-arp-spoofing ip** command to enable gateway-targeted Address Resolution Protocol (ARP) spoofing prevention.

Run the **no** form of this command to disable this feature.

Gateway-targeted ARP spoofing prevention is disabled by default.

Syntax

anti-arp-spoofing ip *ipv4-address*

no anti-arp-spoofing ip *ipv4-address*

Parameter Description

ipv4-address: IPv4 address of the gateway.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command can be configured only on L2 interfaces.

Examples

The following example enables gateway-targeted ARP spoofing prevention on GigabitEthernet 0/1 with the gateway IP address set to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# anti-arp-spoofing ip 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 show anti-arp-spoofing

Function

Run the **show anti-arp-spoofing** command to display data on gateway-targeted ARP spoofing prevention on all interfaces.

Syntax

show anti-arp-spoofing

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays data on gateway-targeted ARP spoofing prevention on all interfaces.

```
Hostname> enable
Hostname# show anti-arp-spoofing
NO    PORT      IP             STATUS
1     Gi0/1     192.168.1.1     active
```

Table 1-1 Output Fields of the show anti-arp-spoofing Command

Field	Description
NO	Serial number
PORT	Port information
IP	Gateway IP address
STATUS	Entry effective status

Notifications

N/A

Platform Description

N/A

Related Commands

- anti-arp-spoofing ip

1 CPP Commands

Command	Function
clear cpu-protect counters	Clear CPP statistics.
clear cpu-protect counters mboard	Clear the CPP statistics on the master device.
clear cpu-protect statistics	Clear the CPP statistics on an interface.
cpu-protect type bandwidth	Configure bandwidth for a specified packet type.
cpu-protect cpu bandwidth	Configure a bandwidth for a CPU port.
cpu-protect intf-statistics enable	Enable the CPP statistics function for a port.
cpu-protect traffic-class bandwidth	Configure a bandwidth for a queue.
cpu-protect type traffic-class	Configure a priority queue for a specified packet type.
show cpu-protect	Display all the configurations and statistics of CPP.
show cpu-protect cpu	Display the configuration of a CPU port.
show cpu-protect mboard	Display all the configurations and statistics of CPP on the master device.
show cpu-protect statistics	Display packet statistics.
show cpu-protect summary	Display all the configurations and statistics of CPP on the master device.
show cpu-protect traffic-class	Display the configurations and statistics of a priority queue.
show cpu-protect type	Display the configurations and statistics of a packet type.

1.1 clear cpu-protect counters

Function

Run the **clear cpu-protect counters** command to clear CPP statistics.

Syntax

clear cpu-protect counters [**device** *device-number*]

Parameter Description

device *device-number*: Specifies the device number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears CPP statistics.

```
Hostname> enable
Hostname# clear cpu-protect counters
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 clear cpu-protect counters mboard

Function

Run the **clear cpu-protect counters mboard** command to clear the CPP statistics on the master device.

Syntax

clear cpu-protect counters mboard

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the CPP statistics on the master device.

```
Hostname> enable
Hostname# clear cpu-protect counters mboard
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.3 clear cpu-protect statistics

Function

Run the **clear cpu-protect statistics** command to clear the CPP statistics on an interface.

Syntax

clear cpu-protect statistics [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the CPP statistics on GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# clear cpu-protect statistics interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.4 cpu-protect type bandwidth

Function

Run the **cpu-protect type bandwidth** command to configure bandwidth for a specified packet type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No bandwidth is configured for a specified packet type by default. Each type of packet has the default bandwidth value.

Syntax

cpu-protect type *packet-type* **bandwidth** *bandwidth-value*

no cpu-**protect type** *packet-type* **bandwidth**

default cpu-**protect type** *packet-type* **bandwidth**

Parameter Description

packet-type: Specified packet type.

bandwidth-value: Configured bandwidth value, in pps. The value range is from 0 to 3000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the bandwidth for BPDU packets to **200** pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu-protect type bpdu bandwitdth 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 cpu-protect cpu bandwidth

Function

Run the **cpu-protect cpu bandwidth** command to configure a bandwidth for a CPU port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The bandwidth for a CPU port is 2250 pps by default.

Syntax

cpu-protect cpu bandwidth *bandwidth-value*

no cpu-protect cpu

default cpu-protect cpu

Parameter Description

bandwidth-value: Configured bandwidth value, in pps. The value range is from 0 to 3000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the bandwidth for a CPU port to **3000** pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu-protect cpu bandwidth 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 cpu-protect intf-statistics enable

Function

Run the **cpu-protect intf-statistics enable** command to enable the CPP statistics function for a port.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The CPP statistics function for any port is disabled by default.

Syntax

cpu-protect intf-statistics enable

no cpu-protect intf-statistics enable

default cpu-protect intf-statistics enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the CPP statistics function on a port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu-protect intf-statistics enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 cpu-protect traffic-class bandwidth

Function

Run the **cpu-protect traffic-class bandwidth** command to configure a bandwidth for a queue.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No bandwidth is configured for a queue by default. Each queue has the default bandwidth value.

Syntax

cpu-protect traffic-class *traffic-class-number* **bandwidth** *bandwidth-value*

no cpu-protect traffic-class *traffic-class-number*

default cpu-protect traffic-class *traffic-class-number*

Parameter Description

traffic-class-number: Specified priority queue. The value range is from 0 to 7.

bandwidth-value: Configured bandwidth value, in pps. The value range is from 0 to 3000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the bandwidth for queue 5 to **2500** pps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu-protect traffic-class 5 bandwidth 2500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 cpu-protect type traffic-class

Function

Run the **cpu-protect type traffic-class** command to configure a priority queue for a specified packet type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Each packet type has the corresponding priority queue by default.

Syntax

cpu-protect type *packet-type* **traffic-class** *traffic-class-number*

no cpu-protect type *packet-type* **traffic-class**

default cpu-protect type *packet-type* **traffic-class**

Parameter Description

packet-type: Specified packet type.

traffic-class-number: Priority queue for a specified packet. The value range is from 0 to 7.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures priority queue 5 for BPDU packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cpu-protect type bpdu traffic-class 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show cpu-protect

Function

Run the **show cpu-protect** command to display all the configurations and statistics of CPP.

Syntax

show cpu-protect [**device** *device-number*]

Parameter Description

device-number: Specified device number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all the configurations and statistics of CPP.

```
Hostname> enable
Hostname# show cpu-protect
%cpu port bandwidth: 100000(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)  Drop(pps)
 0            6000           0         0
 1            6000           0         0
 2            6000           0         0
 3            6000           0         0
 4            6000           0         0
 5            6000           0         0
 6            6000           0         0
 7            6000           0         0
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
Total Drop
bpdu              6            128           0         0         0           0
```

arp	1	3000	0	0	0	0
tpp	6	128	0	0	0	0
dot1x	2	1500	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	5	128	0	0	0	0
lacp	5	256	0	0	0	0
rerp	5	128	0	0	0	0
reup	5	128	0	0	0	0
lldp	5	768	0	0	0	0
cdp	5	768	0	0	0	0
dhcps	2	1500	0	0	0	0
dhcps6	2	1500	0	0	0	0
dhcp6-client	2	1500	0	0	0	0
dhcp6-server	2	1500	0	0	0	0
dhcp-relay-c	2	1500	0	0	0	0
dhcp-relay-s	2	1500	0	0	0	0
option82	2	1500	0	0	0	0
unknown-v6mc	1	128	0	0	0	0
xgv6-ipmc	1	128	0	0	0	0
stargv6-ipmc	1	128	0	0	0	0
unknown-v4mc	1	128	0	0	0	0
xgv-ipmc	2	128	0	0	0	0
stargv-ipmc	2	128	0	0	0	0
udp-helper	1	128	0	0	0	0
dvmrp	4	128	0	0	0	0
igmp	2	1000	0	0	0	0
icmp	3	1600	0	0	0	0
ospf	4	2000	0	0	0	0
ospf3	4	2000	0	0	0	0
pim	4	1000	0	0	0	0
pimv6	4	1000	0	0	0	0
rip	4	128	0	0	0	0
ripng	4	128	0	0	0	0
vrrp	6	256	0	0	0	0
vrrpv6	6	256	0	0	0	0
ttl0	0	128	0	0	0	0
ttl1	0	2000	0	0	0	0
hop-limit	0	800	0	0	0	0
local-ipv4	3	4000	0	0	0	0
local-ipv6	3	4000	0	0	0	0
v4uc-route	1	800	0	0	0	0
v6uc-route	1	800	0	0	0	0
rt-host	4	3000	0	0	0	0
mld	2	1000	0	0	0	0
nd-snp-ns-na	1	3000	0	0	0	0

```
nd-snp-rs          1            1000          0         0         0          0
nd-snp-ra-redirect  1            1000          0         0         0          0
erps               5            128           0         0         0          0
mpls-ttl0          4            128           0         0         0          0
mpls-ttl1          4            128           0         0         0          0
mpls-ctrl          4            128           0         0         0          0
isis               4            2000          0         0         0          0
bgp                4            2000          0         0         0          0
cfm                5            512           0         0         0          0
web-auth           2            2000          0         0         0          0
fcoe-fip           4            1000          0         0         0          0
fcoe-local         4            1000          0         0         0          0
bfd                6            5120          0         0         0          0
micro-bfd          6            5120          0         0         0          0
micro-bfd-v6       6            5120          0         0         0          0
dldp               6            3200          0         0         0          0
other              0            4096          0         0         0          0
trill              4            1000          0         0         0          0
efm                5            1000          0         0         0          0
ipv6-all           0            2000          0         0         0          0
ip-option          0            800           0         0         0          0
mgmt               -            4000          4         0         4639       0
dns                2            200           0         0         0          0
sdn                0            5000          0         0         0          0
sdn_of_fetch       0            5000          0         0         0          0
sdn_of_copy        0            5000          0         0         0          0
sdn_of_trap        0            5000          0         0         0          0
vxlan-non-uc       1            512           0         0         0          0
local-telnet       3            1000          0         0         0          0
local-snmp         3            1000          0         0         0          0
local-ssh          3            1000          0         0         0          0
```

Table 1-1 Output Fields of the show cpu-protect Command

Field	Description
%cpu port bandwidth	Bandwidth for a CPU port
Traffic-class	Priority queue
Bandwidth(pps)	Bandwidth
Rate(pps)	Rate
Drop(pps)	Packet loss rate
Packet Type	Packet type
Total	Total number of received packets

Field	Description
Total Drop	Total number of lost packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show cpu-protect cpu

Function

Run the **show cpu-protect cpu** command to display the configuration of a CPU port.

Syntax

show cpu-protect cpu

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of a CPU port.

```
Hostname> enable
Hostname# show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Table 1-2 Output Fields of the show cpu-protect cpu Command

Field	Description
%cpu port bandwidth	Configured bandwidth of a CPU port

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show cpu-protect mboard

Function

Run the **show cpu-protect mboard** command to display all the configurations and statistics of CPP on the master device.

Syntax

show cpu-protect mboard

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all the configurations and statistics of CPP on the master device.

```
Hostname> enable
Hostname# show cpu-protect mboard
%cpu port bandwidth: 80000(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)      Drop(pps)
 0            8000          0             0
 1            8000          0             0
 2            8000          0             0
 3            8000          0             0
 4            8000          0             0
 5            8000          0             0
 6            8000          0             0
 7            8000          0             0
```

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total Total Drop
bpdu	6	128	0	0	0	0
arp	3	10000	0	0	0	0
arp-dai	3	10000	0	0	0	0
arp-proxy	3	10000	0	0	0	0
tpp	7	128	0	0	0	0
dot1x	4	128	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	6	128	0	0	0	0
lacp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0

```
local-ipv6          6             128             0          0          0          0
route-host-v4       0             4096            0          0          0          0
route-host-v6       0             4096            0          0          0          0
mld                 0             1000            0          0          0          0
nd-snp-ns-na        6             128             0          0          0          0
nd-snp-rs           6             128             0          0          0          0
nd-snp-ra-redirect  6             128             0          0          0          0
nd-non-snp          6             128             0          0          0          0
erps                4             128             0          0          0          0
mpls-ttl0           6             128             0          0          0          0
mpls-ttl1           6             128             0          0          0          0
mpls-ctrl           6             128             0          0          0          0
isis                5             2000            0          0          0          0
bgp                 1             128             0          0          0          0
cfm                 0             128             0          0          0          0
fcoe-fip            6             128             0          0          0          0
fcoe-local          6             128             0          0          0          0
bfd-echo            6             5120            0          0          0          0
bfd-ctrl            6             5120            0          0          0          0
madp                7             1000            0          0          0          0
ip4-other           6             128             0          0          0          0
ip6-other           6             128             0          0          0          0
non-ip-other        6             20000           0          0          0          0
trill               2             1000            0          0          0          0
trill-oam           2             1000            0          0          0          0
efm                 2             1000            0          0          0          0
```

Table 1-3 Output Fields of the show cpu-protect mboard Command

Field	Description
%cpu port bandwidth	Bandwidth for a CPU port
Traffic-class	Priority queue
Bandwidth(pps)	Bandwidth
Rate(pps)	Rate
Drop(pps)	Packet loss rate
Packet Type	Packet type
Total	Total number of received packets
Total Drop	Total number of lost packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show cpu-protect statistics

Function

Run the **show cpu-protect statistics** command to display packet statistics.

Syntax

show cpu-protect statistics { **interface** *interface-type interface-number* | **type** *packet-type* }

Parameter Description

interface *interface-type interface-number*: Displays statistics of a specified interface.

type *packet-type*: Displays the statistics of a specified packet type.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the packet statistics on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show cpu-protect statistics interface gigabitethernet 0/1
Gi0/1
Packet Type        Rate(pps)  Drop(pps)  Total        Total Drop
bpdu              0         0         0           0
arp               0         0         248053       0
tpp               0         0         0           0
dot1x             0         0         0           0
gvrp              0         0         0           0
rldp              0         0         0           0
lacp              0         0         0           0
rerp              0         0         0           0
reup              0         0         0           0
lldp              0         0         560          0
cdp               0         0         0           0
dhcps             0         0         0           0
```

```
dhcps6             0          0          0             0
dhcp6-client       0          0          0             0
dhcp6-server       0          0          0             0
dhcp-relay-c       0          0          0             0
dhcp-relay-s       0          0          0             0
option82           0          0          0             0
unknown-v6mc       0          0          0             0
xgv6-ipmc          0          0          0             0
stargv6-ipmc       0          0          0             0
unknown-v4mc       0          0          0             0
xgv-ipmc           0          0          0             0
stargv-ipmc        0          0          0             0
udp-helper         0          0          0             0
dvmrp              0          0          0             0
igmp               0          0          0             0
icmp               0          0          0             0
ospf               0          0          0             0
ospf3              0          0          0             0
pim                0          0          0             0
pimv6              0          0          0             0
rip                0          0          0             0
ripng              0          0          0             0
vrrp               0          0          0             0
vrrpv6             0          0          0             0
ttl0               0          0          0             0
ttl1               0          0          0             0
hop-limit          0          0          0             0
local-ipv4         0          0          0             0
local-ipv6         0          0          0             0
v4uc-route         0          0          0             0
v6uc-route         0          0          0             0
rt-host            0          0          0             0
mld                0          0          0             0
nd-snp-ns-na       0          0          0             0
nd-snp-rs          0          0          0             0
nd-snp-ra-redirect 0          0          0             0
erps               0          0          0             0
mpls-ttl0          0          0          0             0
mpls-ttl1          0          0          0             0
mpls-ctrl          0          0          0             0
isis               0          0          0             0
bgp                0          0          0             0
cfm                0          0          0             0
web-auth           0          0          0             0
fcoe-fip           0          0          0             0
fcoe-local         0          0          0             0
```

```
bfd              0         0         0           0
micro-bfd         0         0         0           0
micro-bfd-v6      0         0         0           0
dldp             0         0         0           0
other            0         0         0           0
trill            0         0         0           0
efm              0         0         0           0
ipv6-all          0         0         0           0
ip-option         0         0         0           0
mgmt             0         0         0           0
dns              0         0         0           0
sdn              0         0         0           0
sdn_of_fetch      0         0         0           0
sdn_of_copy       0         0         0           0
sdn_of_trap       0         0         0           0
vxlan-non-uc      0         0         0           0
```

Table 1-4 Output Fields of the show cpu-protect statistics Command

Field	Description
Rate(pps)	Rate
Drop(pps)	Packet loss rate
Packet Type	Packet type
Total	Total number of packets
Total Drop	Total number of lost packets
Interface	Interface name

The following example displays the configurations and statistics of ARP packets on the master device.

```
Hostname> enable
Hostname# show cpu-protect statistics type arp
arp
Interface         Rate(pps)  Drop(pps)  Total        Total Drop
Te0/33           0         0         248053       0
Te0/34           0         0         0           0
Te0/35           0         0         0           0
Te0/36           0         0         0           0
```

Notifications

N/A

Related Commands

N/A

1.13 show cpu-protect summary

Function

Run the **show cpu-protect summary** command to display all the configurations and statistics of CPP on the master device.

Syntax

show cpu-protect summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all the configurations and statistics of CPP on the master device.

```
Hostname> enable
Hostname# show cpu-protect summary
%cpu port bandwidth: 100000(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)  Drop(pps)
 0            6000          0         0
 1            6000          0         0
 2            6000          0         0
 3            6000          0         0
 4            6000          0         0
 5            6000          0         0
 6            6000          0         0
 7            6000          0         0
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
Total Drop
bpdu              6            128           0         0         0           0
arp               1            3000          0         0         0           0
tpp               6            128           0         0         0           0
dot1x             2            1500          0         0         0           0
gvrp              5            128           0         0         0           0
```

rldp	5	128	0	0	0	0
lacp	5	256	0	0	0	0
rerp	5	128	0	0	0	0
reup	5	128	0	0	0	0
lldp	5	768	0	0	0	0
cdp	5	768	0	0	0	0
dhcps	2	1500	0	0	0	0
dhcps6	2	1500	0	0	0	0
dhcp6-client	2	1500	0	0	0	0
dhcp6-server	2	1500	0	0	0	0
dhcp-relay-c	2	1500	0	0	0	0
dhcp-relay-s	2	1500	0	0	0	0
option82	2	1500	0	0	0	0
unknown-v6mc	1	128	0	0	0	0
xgv6-ipmc	1	128	0	0	0	0
stargv6-ipmc	1	128	0	0	0	0
unknown-v4mc	1	128	0	0	0	0
xgv-ipmc	2	128	0	0	0	0
stargv-ipmc	2	128	0	0	0	0
udp-helper	1	128	0	0	0	0
dvmrp	4	128	0	0	0	0
igmp	2	1000	0	0	0	0
icmp	3	1600	0	0	0	0
ospf	4	2000	0	0	0	0
ospf3	4	2000	0	0	0	0
pim	4	1000	0	0	0	0
pimv6	4	1000	0	0	0	0
rip	4	128	0	0	0	0
ripng	4	128	0	0	0	0
vrrp	6	256	0	0	0	0
vrrpv6	6	256	0	0	0	0
ttl0	0	128	0	0	0	0
ttl1	0	2000	0	0	0	0
hop-limit	0	800	0	0	0	0
local-ipv4	3	4000	0	0	0	0
local-ipv6	3	4000	0	0	0	0
v4uc-route	1	800	0	0	0	0
v6uc-route	1	800	0	0	0	0
rt-host	4	3000	0	0	0	0
mld	2	1000	0	0	0	0
nd-snp-ns-na	1	3000	0	0	0	0
nd-snp-rs	1	1000	0	0	0	0
nd-snp-ra-redirect	1	1000	0	0	0	0
erps	5	128	0	0	0	0
mpls-ttl0	4	128	0	0	0	0
mpls-ttl1	4	128	0	0	0	0

```
mpls-ctrl          4            128           0          0          0          0
isis               4           2000           0          0          0          0
bgp                4           2000           0          0          0          0
cfm                5            512           0          0          0          0
web-auth           2           2000           0          0          0          0
fcoe-fip           4           1000           0          0          0          0
fcoe-local         4           1000           0          0          0          0
bfd                6           5120           0          0          0          0
micro-bfd          6           5120           0          0          0          0
micro-bfd-v6       6           5120           0          0          0          0
dldp               6           3200           0          0          0          0
other              0           4096           0          0          0          0
trill              4           1000           0          0          0          0
efm                5           1000           0          0          0          0
ipv6-all           0           2000           0          0          0          0
ip-option          0            800           0          0          0          0
mgmt               -           4000           4          0       4639          0
dns                2            200           0          0          0          0
sdn                0           5000           0          0          0          0
sdn_of_fetch       0           5000           0          0          0          0
sdn_of_copy        0           5000           0          0          0          0
sdn_of_trap        0           5000           0          0          0          0
vxlan-non-uc       1            512           0          0          0          0
local-telnet       3           1000           0          0          0          0
local-snmp         3           1000           0          0          0          0
local-ssh          3           1000           0          0          0          0
```

Table 1-5 Output Fields of the show cpu-protect summary Command

Field	Description
%cpu port bandwidth	Bandwidth for a CPU port
Traffic-class	Priority queue
Bandwidth(pps)	Bandwidth
Rate(pps)	Rate
Drop(pps)	Packet loss rate
Packet Type	Packet type
Total	Total number of received packets
Total Drop	Total number of lost packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show cpu-protect traffic-class

Function

Run the **show cpu-protect traffic-class** command to display the configurations and statistics of a priority queue.

Syntax

show cpu-protect traffic-class { **all** | *traffic-class-number* } [**device** *device-number*]

Parameter Description

all: Displays all priority queue information.

traffic-class-number: Information of a specified priority queue. The value range is from 0 to 7.

device *device-number*: Specifies the device number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configurations and statistics of all priority queues on the master device.

```
Hostname> enable
Hostname# show cpu-protect traffic-class all
Traffic-class   Bandwidth(pps)  Rate(pps)      Drop(pps)
 0            8000          0             0
 1            8000          0             0
 2            8000          0             0
 3            8000          0             0
 4            8000          0             0
 5            3200          0             0
 6            8000          0             0
 7            8000          0             0
```

Table 1-6 Output Fields of the show cpu-protect traffic-class Command

Field	Description
Traffic-class	Priority queue
Bandwidth(pps)	Bandwidth
Rate(pps)	Rate
Drop(pps)	Packet loss rate

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show cpu-protect type

Function

Run the **show cpu-protect type** command to display the configurations and statistics of a packet type.

Syntax

show cpu-protect type *packet-type* [**device** *device-number*]

Parameter Description

packet-type: Specified packet type.

device *device-number*: Specifies the device number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configurations and statistics of ICMP packets on the master device.

```
Hostname> enable
Hostname# show cpu-protect type icmp
```

```
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
Total Drop
icmp               5              1500            50         0          10000    100
```

Table 1-7 Output Fields of the show cpu-protect type Command

Field	Description
Traffic-class	Priority queue
Bandwidth(pps)	Bandwidth
Rate(pps)	Rate
Drop(pps)	Packet loss rate
Packet Type	Packet type
Total	Total number of received packets
Total Drop	Total number of lost packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 NFPP Commands

Command	Function
all-guard enable	Enable all the basic types of global guard of Network Foundation Protection Policy (NFPP).
arp-guard attack-threshold	Configure the global attack threshold of ARP guard.
arp-guard enable	Enable the function of global ARP guard.
arp-guard isolate-forwarding enable	Enable the function of global isolation forwarding of ARP guard.
arp-guard isolate-period	Configure the global isolation time of ARP guard.
arp-guard monitored-host-limit	Configure the maximum number of monitored hosts of ARP guard in global configuration mode.
arp-guard monitor-period	Configure the monitoring time of ARP guard.
arp-guard rate-limit	Configure the global rate limiting threshold of ARP guard.
arp-guard ratelimit-forwarding enable	Enable the function of port-based rate limit forwarding of ARP guard.
arp-guard scan-threshold	Configure the global scanning threshold of ARP guard.
clear nfpp arp-guard hosts	Clear the monitored hosts of ARP guard.
clear nfpp arp-guard scan	Clear the scanning table of ARP guard.
clear nfpp define hosts	Clear the monitored hosts of the customized guard type.
clear nfpp dhcp-guard hosts	Clear the monitored hosts of DHCP guard.
clear nfpp dhcpv6-guard hosts	Clear the monitored hosts of DHCPv6 guard.
clear nfpp icmp-guard hosts	Clear the monitored hosts of ICMP guard.
clear nfpp ip-guard hosts	Clear the monitored hosts of IP guard.
clear nfpp log	Clear the log buffer of NFPP.
clear nfpp nd-guard hosts	Clear the monitored hosts of ND guard.
clear nfpp tcp-syn-guard hosts	Clear the monitored hosts of TCP-SYN guard.

define	Customize a guard type and enter the customized guard configuration mode of NFPP.
define enable	Enable the function of global customized guard.
dhcp-guard attack-threshold	Configure the global attack threshold of DHCP guard.
dhcp-guard enable	Enable the function of global DHCP guard.
dhcp-guard isolate-period	Configure the global isolation time of DHCP guard.
dhcp-guard monitored-host-limit	Configure the maximum number of monitored hosts of DHCP guard.
dhcp-guard monitor-period	Configure the monitoring time of DHCP guard.
dhcp-guard rate-limit	Configure the global rate limiting threshold of DHCP guard.
dhcpv6-guard attack-threshold	Configure the global attack threshold of DHCPv6 guard.
dhcpv6-guard enable	Enable the DHCPv6 guard function.
dhcpv6-guard monitored-host-limit	Configure the maximum number of monitored hosts of DHCPv6 guard.
dhcpv6-guard monitor-period	Configure the monitoring time of DHCPv6 guard.
dhcpv6-guard rate-limit	Configure the global rate limiting threshold of DHCPv6 guard.
global-policy	Configure the global rate limiting threshold and global attack threshold of the customized guard type.
icmp-guard attack-threshold	Configure the global attack threshold of ICMP guard.
icmp-guard enable	Enable the function of global ICMP guard.
icmp-guard isolate-period	Configure the global isolation time of ICMP guard.
icmp-guard monitored-host-limit	Configure the maximum number of monitored hosts of ICMP guard.
icmp-guard monitor-period	Configure the monitoring time of ICMP guard.
icmp-guard rate-limit	Configure the global rate limiting threshold of ICMP guard.
icmp-guard trusted-host	Configure the trusted hosts of ICMP guard.
ip-guard attack-threshold	Configure the global attack threshold of IP guard.

nfpp arp-guard scan-threshold	Configure the scanning threshold of ARP guard on an interface.
nfpp define enable	Enable the customized guard function on an interface.
nfpp define policy	Configure a local rate limiting threshold and a local attack threshold of customized guard on an interface.
nfpp dhcp-guard enable	Enable the DHCP guard function on an interface.
nfpp dhcp-guard isolate-period	Configure the local isolation time of DHCP guard on an interface.
nfpp dhcp-guard policy	Configure a local rate limiting threshold and a local attack threshold of DHCP guard on an interface.
nfpp dhcpv6-guard enable	Enable the DHCPv6 guard function on an interface.
nfpp dhcpv6-guard policy	Configure a local rate limiting threshold and a local attack threshold of DHCPv6 guard on an interface.
nfpp icmp-guard enable	Enable the ICMP guard function on an interface.
nfpp icmp-guard isolate-period	Configure the local isolation time of ICMP guard on an interface.
nfpp icmp-guard policy	Configure a local rate limiting threshold and a local attack threshold of ICMP guard on an interface.
nfpp ip-guard enable	Enable the IP guard function on an interface.
nfpp ip-guard isolate-period	Configure the local isolation time of IP guard on an interface.
nfpp ip-guard policy	Configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.
nfpp ip-guard scan-threshold	Configure the local scanning threshold of IP guard on an interface.
nfpp nd-guard enable	Enable the ND guard function on an interface.
nfpp nd-guard policy per-port	Configure a local rate limiting threshold and a local attack threshold of ND guard on an interface.
nfpp tcp-syn-guard enable	Enable the TCP-SYN guard function on an interface.
nfpp tcp-syn-guard isolate-period	Configure the local isolation time of TCP-SYN guard on an interface.

nfpp tcp-syn-guard policy	Configure a local rate limiting threshold and a local attack threshold of TCP-SYN guard on an interface.
show nfpp arp-guard hosts	Display the monitored hosts of ARP guard.
show nfpp arp-guard scan	Display the scanning table of ARP guard.
show nfpp arp-guard summary	Display the configuration information of ARP guard.
show nfpp define hosts	Display the monitored hosts of a customized guard type.
show nfpp define summary	Display the configuration information of a customized summary type.
show nfpp define trusted-host	Display the trusted hosts of a customized guard type.
show nfpp dhcp-guard hosts	Display the monitored hosts of DHCP guard.
show nfpp dhcp-guard summary	Display the configuration information of DHCP guard.
show nfpp dhcpv6-guard hosts	Display the monitored hosts of DHCPv6 guard.
show nfpp dhcpv6-guard summary	Display the configuration information of DHCPv6 guard.
show nfpp icmp-guard hosts	Display the monitored hosts of ICMP guard.
show nfpp icmp-guard summary	Display the configuration information of ICMP guard.
show nfpp icmp-guard trusted-host	Display the trusted hosts of ICMP guard.
show nfpp ip-guard hosts	Display the monitored hosts of IP guard.
show nfpp ip-guard summary	Display the configuration information of IP guard.
show nfpp ip-guard trusted-host	Display the trusted hosts of IP guard.
show nfpp log buffer	Display the information in the log buffer of NFPP.
show nfpp log buffer statistics	Display the statistics about the log buffer of NFPP.
show nfpp log summary	Display the configuration information of NFPP logs.
show nfpp nd-guard hosts	Display the monitored hosts of ND guard.
show nfpp nd-guard summary	Display the configuration information of ND guard.
show nfpp tcp-syn-guard hosts	Display the monitored hosts of TCP-SYN guard.
show nfpp tcp-syn-guard summary	Display the configuration information of TCP-SYN guard.

show nfpp tcp-syn-guard trusted-host	Display the trusted hosts of TCP-SYN guard.
tcp-syn-guard attack-threshold	Configure the global attack threshold of TCP-SYN guard.
tcp-syn-guard enable	Enable the global TCP-SYN guard function.
tcp-syn-guard isolate-period	Configure the global isolation time of TCP-SYN guard.
tcp-syn-guard monitored-host-limit	Configure the maximum number of monitored hosts of TCP-SYN guard.
tcp-syn-guard monitor-period	Configure the monitoring time of TCP-SYN guard.
tcp-syn-guard rate-limit	Configure the global rate limiting threshold of TCP-SYN guard.
tcp-syn-guard trusted-host	Configure the trusted hosts of TCP-SYN guard.
trusted-host	Configure trusted hosts of a customized guard type.

1.1 all-guard enable

Function

Run the **all-guard enable** command to enable all the basic types of global guard of Network Foundation Protection Policy (NFPP).

Run the **no** form of this command to disable this feature.

Syntax

all-guard enable

no all-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The preceding two commands cannot be displayed by running the **show running-config** command.

This global disabling/enabling command is supported on the basic types of global guard, including ARP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.

This command is not supported on global customized guard types and does not affect the enabling status of the guard type in interface configuration mode.

This command cannot be saved, but its running result can be saved and take effect after device restart.

If you have configured the function of ARP source suppression and the isolation time for the IP guard function in global or interface configuration mode, an error is reported when you enable the IP guard function.

Examples

The following example disables all the basic types of global guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# no all-guard enable
```

Notifications

If you have configured the function of ARP source suppression, the following notification will be displayed when you configure isolation time for IP guard:

```
Configuration is prohibited, please disable the arp-guard suppression function first!
```

Common Errors

N/A

Related Commands

N/A

1.2 arp-guard attack-threshold

Function

Run the **arp-guard attack-threshold** command to configure the global attack threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ARP guard for each interface is 200 pps, for each source IP address is 100 pps, and for each source MAC address is 100 pps.

Syntax

arp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* | **per-src-mac** *attack-threshold* }

no arp-guard attack-threshold { **per-port** | **per-src-ip** | **per-src-mac** }

default arp-guard attack-threshold { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs. The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the global attack thresholds of ARP guard to **50** pps, **2** pps, and **3** pps for each interface, source IP address, and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard attack-threshold per-port 50
```

```
Hostname(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# arp-guard attack-threshold per-src-mac 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 arp-guard enable

Function

Run the **arp-guard enable** command to enable the function of global ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ARP guard is enabled by default.

Syntax

arp-guard enable

no arp-guard enable

default arp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
```

```
Hostname(config-nfpp)# arp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 arp-guard isolate-forwarding enable

Function

Run the **arp-guard isolate-forwarding enable** command to enable the function of global isolation forwarding of ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global isolation forwarding of ARP guard is enabled by default.

Syntax

arp-guard isolate-forwarding enable

no arp-guard isolate-forwarding enable

default arp-guard isolate-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global isolation forwarding of ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
```

```
Hostname(config-nfpp)# arp-guard isolate-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 arp-guard isolate-period

Function

Run the **arp-guard isolate-period** command to configure the global isolation time of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of ARP guard is **0**.

Syntax

arp-guard isolate-period { *interval* | **permanent** }

no arp-guard isolate-period

default arp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global isolation time of ARP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 arp-guard monitored-host-limit

Function

Run the **arp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of ARP guard in global configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of ARP guard in global configuration mode is **20000** by default.

Syntax

arp-guard monitored-host-limit *limit-number*

no arp-guard monitored-host-limit

default arp-guard monitored-host-limit

Parameter Description

limit-number: Maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_ARP_GUARD-SESSION_LIMIT: Attempt to exceed limit of ARP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of ARP guard in global configuration mode to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 arp-guard monitor-period

Function

Run the **arp-guard monitor-period** command to configure the monitoring time of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of ARP guard is **600** seconds.

Syntax

arp-guard monitor-period *interval*

no arp-guard monitor-period

default arp-guard monitor-period

Parameter Description

interval: Monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When an attacker is detected, if the isolation time is 0, the attacker is monitored through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of ARP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 arp-guard rate-limit

Function

Run the **arp-guard rate-limit** command to configure the global rate limiting threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ARP guard for each interface is 128 pps, for each source IP address is 30 pps, and for each source MAC address is 30 pps.

Syntax

arp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* | **per-src-mac** *rate-limit* }

no arp-guard rate-limit { **per-port** | **per-src-ip** | **per-src-mac** }

default arp-guard rate-limit { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ARP guard to **50** pps, **2** pps, and **3** pps for each interface, source IP address, and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard rate-limit per-port 50
Hostname(config-nfpp)# arp-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# arp-guard rate-limit per-src-mac 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 arp-guard ratelimit-forwarding enable

Function

Run the **arp-guard ratelimit-forwarding enable** command to enable the function of port-based rate limit forwarding of ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of port-based rate limit forwarding of ARP guard is disabled by default.

Syntax

arp-guard ratelimit-forwarding enable

no arp-guard ratelimit-forwarding enable

default arp-guard ratelimit-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of port-based rate limiting forwarding of ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 arp-guard scan-threshold

Function

Run the **arp-guard scan-threshold** command to configure the global scanning threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global scanning threshold of ARP guard is 100 packets per 10 seconds by default.

Syntax

arp-guard scan-threshold *scan-threshold*

no arp-guard scan-threshold

default arp-guard scan-threshold

Parameter Description

scan-threshold: Scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

For the ARP packets received within 10 seconds beyond the scanning threshold, if the source MAC address is unchanged and the source IP address is changing on the link layer, or the source MAC address and source IP address on the link layer are unchanged but the destination IP address is changing, a scanning attack is suspected.

Examples

The following example sets the global scanning threshold of ARP guard to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 clear nfpp arp-guard hosts

Function

Run the **clear nfpp arp-guard hosts** command to clear the monitored hosts of ARP guard.

Syntax

clear nfpp arp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The isolated hosts must be released.

Examples

The following example clears the monitored hosts of ARP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp arp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 clear nfpp arp-guard scan

Function

Run the **clear nfpp arp-guard scan** command to clear the scanning table of ARP guard.

Syntax

clear nfpp arp-guard scan

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the scanning table of ARP guard.

```
Hostname> enable
Hostname# clear nfpp arp-guard scan
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 clear nfpp define hosts

Function

Run the **clear nfpp define hosts** command to clear the monitored hosts of the customized guard type.

Syntax

clear nfpp define *define-name* **hosts** [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address* | *ipv6-address*] *]

Parameter Description

define-name: Specified customized guard type.

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

mac-address: Specified MAC address of a monitored host to be cleared.

ipv6-address: Specified IPv6 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The isolated hosts must be released.

If this command is run without parameters, all monitored hosts of this customized type are cleared.

Examples

The following example clears the monitored hosts of the customized TCP guard type on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp define tcp hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 clear nfpp dhcp-guard hosts

Function

Run the **clear nfpp dhcp-guard hosts** command to clear the monitored hosts of DHCP guard.

Syntax

clear nfpp dhcp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all isolated hosts are cleared.

Examples

The following example clears the monitored hosts of DHCP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp dhcp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 clear nfpp dhcpv6-guard hosts

Function

Run the **clear nfpp dhcpv6-guard hosts** command to clear the monitored hosts of DHCPv6 guard.

Syntax

clear nfpp dhcpv6-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all isolated hosts are cleared.

Examples

The following example clears the monitored hosts of DHCPv6 guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp dhcpv6-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 clear nfpp icmp-guard hosts

Function

Run the **clear nfpp icmp-guard hosts** command to clear the monitored hosts of ICMP guard.

Syntax

clear nfpp icmp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of ICMP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp icmp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 clear nfpp ip-guard hosts

Function

Run the **clear nfpp ip-guard hosts** command to clear the monitored hosts of IP guard.

Syntax

clear nfpp ip-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of IP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp ip-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.18 clear nfpp log

Function

Run the **clear nfpp log** command to clear the log buffer of NFPP.

Syntax

clear nfpp log

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the log buffer of NFPP.

```
Hostname> enable
Hostname# clear nfpp log
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.19 clear nfpp nd-guard hosts

Function

Run the **clear nfpp nd-guard hosts** command to clear the monitored hosts of ND guard.

Syntax

clear nfpp nd-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

If a host is configured with a rate limiting threshold by hardware, this configuration must be cleared.

Examples

The following example clears the monitored hosts of ND guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp nd-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 clear nfpp tcp-syn-guard hosts

Function

Run the **clear nfpp tcp-syn-guard hosts** command to clear the monitored hosts of TCP-SYN guard.

Syntax

clear nfpp tcp-syn-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of TCP-SYN guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp tcp-syn-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 define

Function

Run the **define** command to customize a guard type and enter the customized guard configuration mode of NFPP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Syntax

define *define-name*

no define *define-name*

default define *define-name*

Parameter Description

define-name: Name of a customized guard type.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates a customized guard type named TCP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 define enable

Function

Run the **define enable** command to enable the function of global customized guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global customized guard is disabled by default.

Syntax

define *define-name* **enable**

no define *define-name* **enable**

default define *define-name* **enable**

Parameter Description

define-name: Name of an enabled customized guard function.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To validate the configuration of this command, you must configure the **match**, **rate-limit**, and **attack-threshold** parameters for this command.

Examples

The following example enables the global guard function of the TCP type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 dhcp-guard attack-threshold

Function

Run the **dhcp-guard attack-threshold** command to configure the global attack threshold of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of DHCP guard for each interface is 256 pps, and for each source MAC address is 10 pps.

Syntax

dhcp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

no dhcp-guard attack-threshold { **per-port** | **per-src-mac** }

default dhcp-guard attack-threshold { **per-port** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs.

Examples

The following example sets the global attack thresholds of DHCP guard to **200** pps and **15** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard attack-threshold per-port 200
Hostname(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 dhcp-guard enable

Function

Run the **dhcp-guard enable** command to enable the function of global DHCP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global DHCP guard is enabled by default.

Syntax

dhcp-guard enable

no dhcp-guard enable

default dhcp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global DHCP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 dhcp-guard isolate-period

Function

Run the **dhcp-guard isolate-period** command to configure the global isolation time of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of DHCP guard is **0**.

Syntax

dhcp-guard isolate-period { *interval* | **permanent** }

no dhcp-guard isolate-period

default dhcp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Isolation time of attackers falls into global isolation time and port-based isolation time (or local isolation time). If no port-based isolation time is configured for an interface, the global isolation time applies.

Examples

The following example sets the global isolation time of DHCP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 dhcp-guard monitored-host-limit

Function

Run the **dhcp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of DHCP guard is **20000** by default.

Syntax

dhcp-guard monitored-host-limit *number*

no dhcp-guard monitored-host-limit

default dhcp-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DHCP_GUARD-SESSION_LIMIT: Attempt to exceed limit of DHCP 20000 monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of DHCP guard to **200**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 dhcp-guard monitor-period

Function

Run the **dhcp-guard monitor-period** command to configure the monitoring time of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of DHCP guard is **600** seconds.

Syntax

dhcp-guard monitor-period *interval*

no dhcp-guard monitor-period

default dhcp-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When DHCP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of DHCP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 dhcp-guard rate-limit

Function

Run the **dhcp-guard rate-limit** command to configure the global rate limiting threshold of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of DHCP guard for each interface is 150 pps, and for each source MAC address is 5 pps.

Syntax

dhcp-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

no dhcp-guard rate-limit { **per-port** | **per-src-mac** }

default dhcp-guard rate-limit { **per-port** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global attack thresholds of DHCP guard to **100** pps and **8** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard rate-limit per-port 100
Hostname(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 dhcpv6-guard attack-threshold

Function

Run the **dhcpv6-guard attack-threshold** command to configure the global attack threshold of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of DHCPv6 guard for each interface is 256 pps, and for each source MAC address is 10 pps.

Syntax

dhcpv6-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

no dhcpv6-guard attack-threshold { **per-port** | **per-src-mac** }

default dhcpv6-guard attack-threshold { **per-port** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs.

Examples

The following example sets the global attack thresholds of DHCPv6 guard to **200** pps and **15** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 dhcpv6-guard enable

Function

Run the **dhcpv6-guard enable** command to enable the DHCPv6 guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCPv6 guard function is enabled by default.

Syntax

dhcpv6-guard enable

no dhcpv6-guard enable

default dhcpv6-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global DHCPv6 guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 dhcpv6-guard monitored-host-limit

Function

Run the **dhcpv6-guard monitored-host-limit** command to configure the maximum number of monitored hosts of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of DHCPv6 guard is **20000** by default.

Syntax

dhcpv6-guard monitored-host-limit *number*

no dhcpv6-guard monitored-host-limit

default dhcpv6-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DHCPV6_GUARD -SESSION_LIMIT: Attempt to exceed limit of DHCPv6 20000 monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of DHCPv6 guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 dhcpv6-guard monitor-period

Function

Run the **dhcpv6-guard monitor-period** command to configure the monitoring time of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of DHCPv6 guard is **600** seconds.

Syntax

dhcpv6-guard monitor-period *interval*

no dhcpv6-guard monitor-period

default dhcpv6-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When DHCPv6 guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of DHCPv6 guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 dhcpv6-guard rate-limit

Function

Run the **dhcpv6-guard rate-limit** command to configure the global rate limiting threshold of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of DHCPv6 guard for each interface is 150 pps, and for each source MAC address is 5 pps.

Syntax

dhcpv6-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

no dhcpv6-guard rate-limit { **per-port** | **per-src-mac** }

default dhcpv6-guard rate-limit { **per-port** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting threshold of DHCPv6 guard to **100** pps and **8** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-port 100
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 global-policy

Function

Run the **global-policy** command to configure the global rate limiting threshold and global attack threshold of the customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No global rate limiting threshold and global attack threshold of the customized guard type are configured by default.

Syntax

global-policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no global-policy { **per-port** | **per-src-ip** | **per-src-mac** }

default global-policy { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port: Performs rate statistics based on the physical port that receives packets.

per-src-ip: Performs rate statistics based on the source IP address, VLAN ID, and port that are used to identify hosts.

per-src- mac: Performs rate statistics based on the source MAC address, VLAN ID, and port that are used to identify hosts.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

To create a customized guard type, you must specify rules of rate statistics classification for this type. You must identify hosts based on the source IP address and source MAC address, perform customized packet rate statistics based on the users, or perform rate statistics based on ports and specify rate limiting thresholds and attack thresholds for different classes of rate statistics. The attack threshold must be equal to or greater than the rate limiting threshold. When the rate exceeds the rate limiting threshold, packets of the customized type in this class are discarded. When the rate exceeds the attack threshold, an attack occurs, a log is printed, and a Trap message is sent.

Examples

The following example configures the customized guard type as TCP, sets the global rate limiting threshold and global attack threshold for each interface to **100** pps and **200** pps, and sets the global rate limiting threshold and global attack threshold for each source IP address to **10** pps and **20** pps respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# global-policy per-port 100 200
Hostname(config-nfpp-define)# global-policy per-src-ip 10 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 icmp-guard attack-threshold

Function

Run the **icmp-guard attack-threshold** command to configure the global attack threshold of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ICMP guard for each interface is 400 pps, and for each source IP address is 300 pps.

Syntax

icmp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no icmp-guard attack-threshold { **per-port** | **per-src-ip** }

default icmp-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global attack thresholds of ICMP guard to **1200** pps and **600** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard attack-threshold per-port 1200
Hostname(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 icmp-guard enable

Function

Run the **icmp-guard enable** command to enable the function of global ICMP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ICMP guard is enabled by default.

Syntax

icmp-guard enable

no icmp-guard enable

default icmp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ICMP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 icmp-guard isolate-period

Function

Run the **icmp-guard isolate-period** command to configure the global isolation time of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form this command to restore the default configuration.

The default global isolation time of ICMP guard is **0**.

Syntax

icmp-guard isolate-period { *interval* | **permanent** }

no icmp-guard isolate-period

default icmp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Isolation time of attackers falls into global isolation time and port-based isolation time (or local isolation time). If no port-based isolation time is configured for an interface, the global isolation time applies.

Examples

The following example sets the global isolation time of ICMP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 icmp-guard monitored-host-limit

Function

Run the **icmp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts is **20000** by default.

Syntax

icmp-guard monitored-host-limit *number*

no icmp-guard monitored-host-limit

default icmp-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_ICMP_GUARD-SESSION_LIMIT: Attempt to exceed limit of ICMP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of ICMP guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 icmp-guard monitor-period

Function

Run the **icmp-guard monitor-period** command to configure the monitoring time of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of ICMP guard is **600** seconds.

Syntax

icmp-guard monitor-period *interval*

no icmp-guard monitor-period

default icmp-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When ICMP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of ICMP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 icmp-guard rate-limit

Function

Run the **icmp-guard rate-limit** command to configure the global rate limiting threshold of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ICMP guard for each interface is 250 pps, and for each source IP address is 200 pps.

Syntax

icmp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no icmp-guard rate-limit { **per-port** | **per-src-ip** }

default icmp-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ICMP guard to **800** pps and **500** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard rate-limit per-port 800
Hostname(config-nfpp)# icmp-guard rate-limit per-src-ip 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 icmp-guard trusted-host

Function

Run the **icmp-guard trusted-host** command to configure the trusted hosts of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host by default.

Syntax

icmp-guard trusted-host *ipv4-address mask*

no icmp-guard trusted-host { *ipv4-address mask* | **all** }

default icmp-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, ICMP packets sent by this host can be forwarded to the CPU without rate limit or alarm. All hosts in a network segment can be configured as trusted hosts by configuring a mask.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of ICMP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 ip-guard attack-threshold

Function

Run the **ip-guard attack-threshold** command to configure the global attack threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of IP guard for each interface is 200 pps, and for each source IP address is 100 pps.

Syntax

ip-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no ip-guard attack-threshold { **per-port** | **per-src-ip** }

default ip-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

IP guard is to solve IP attacks whose destination IP address is not a local IP address. If the destination IP address is a local IP address, the rates of IP packets are limited by the function of CPU protect policy (CPP).

Examples

The following example sets the global attack thresholds of IP guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard attack-threshold per-port 50
Hostname(config-nfpp)# ip-guard attack-threshold per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 ip-guard enable

Function

Run the **ip-guard enable** command to enable the global IP guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The global IP guard function is enabled by default.

Syntax

ip-guard enable

no ip-guard enable

default ip-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global IP guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard enable
```

Notifications

No notification can be configured.

```
Configuration is prohibited, please disable the arp-guard suppression function first!
```

Common Errors

If you have configured the function of ARP source suppression and the isolation time for IP guard in global or interface configuration mode, an error is reported when you enable the function of global IP guard.

Platform Description

N/A

Related Commands

N/A

1.44 ip-guard isolate-period

Function

Run the **ip-guard isolate-period** command to configure the global isolation time of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of IP guard is **0**.

Syntax

ip-guard isolate-period { *interval* | **permanent** }

no ip-guard isolate-period

default ip-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

If you have configured the function of ARP source suppression, you are not allowed to configure the isolation function unless you disable the function of ARP source suppression.

Examples

The following example sets the global isolation time of IP guard to **180** seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard isolate-period 180
```

Notifications

If you have configured the ARP source suppression function, the following notification will be displayed when you configure isolation time for the IP guard function:

```
Configuration is prohibited, please disable the arp-guard suppression function first!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 ip-guard monitored-host-limit

Function

Run the **ip-guard monitored-host-limit** command to configure the maximum number of monitored hosts of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of IP guard is **20000** by default.

Syntax

ip-guard monitored-host-limit *number*

no ip-guard monitored-host-limit

default ip-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of

monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to delete clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_IP_GUARD-SESSION_LIMIT: Attempt to exceed limit of IP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of IP guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 ip-guard monitor-period

Function

Run the **ip-guard monitor-period** command to configure the monitoring time of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of IP guard is **600** seconds.

Syntax

ip-guard monitor-period *interval*

no ip-guard monitor-period

default ip-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When IP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of IP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 ip-guard rate-limit

Function

Run the **ip-guard rate-limit** command to configure the global rate limiting threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of IP guard for each interface is 50 pps, and for each source IP address is 20 pps.

Syntax

ip-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no ip-guard rate-limit { **per-port** | **per-src-ip** }

default ip-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of IP guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard rate-limit per-port 50
Hostname(config-nfpp)# ip-guard rate-limit per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.48 ip-guard scan-threshold

Function

Run the **ip-guard scan-threshold** command to configure the global scanning threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global scanning threshold of IP guard is 100 packets per 10 seconds by default.

Syntax

ip-guard scan-threshold *scan-threshold*

no ip-guard scan-threshold

default ip-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global scanning threshold of IP guard to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 ip-guard trusted-host

Function

Run the **ip-guard trusted-host** command to configure the trusted hosts of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of IP guard by default.

Syntax

ip-guard trusted-host *ipv4-address mask*

no ip-guard trusted-host { *ipv4-address mask* | **all** }

default ip-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, IP packets sent by this host can be forwarded to the CPU without rate limit or alarm.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of IP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)#ip-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 log-buffer enable

Function

Run the **log-buffer enable** command to enable the function of screen log output.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of screen log output is disabled by default and logs are saved in the buffer.

Syntax

log-buffer enable

no log-buffer enable

default log-buffer enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Full scanning table of ARP entries and session oversize are directly output on the screen without limit by the following rules.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to **0**:

- If the **log-buffer enable** command is also configured, logs are output onto the screen without limit.
- If the **log-buffer enable** command is not configured, the logs related to isolation and port rate limit are output onto the screen without limit by the **log-buffer logs** command and other types of logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to **0** and the value of *interval* to a none-zero value: Logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the values of the *message-number* and *interval* parameters to none-zero values:

- If the **log-buffer enable** command is configured, logs are first stored in the log buffer and then output onto the screen regularly based on the *interval* configuration.
- If the **log-buffer enable** command is not configured, logs are first stored in the log buffer, and logs related to isolation and port rate limit are output onto the screen regularly based on the *interval* configuration.

When logs are first output onto the screen, the historical logs in the log buffer are output onto the screen. Before starting the configuration, you are advised to run the **clear nfpp log** command to clear the logs in the log buffer.

After active/standby switchover of a device, the device will clear logs in a buffer and record new logs again.

Examples

The following example enables the function of screen log output.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 log-buffer entries

Function

Run the **log-buffer entries** command to configure the size of the log buffer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default size of the NFPP log buffer is **256** pieces.

Syntax

log-buffer entries *number*

no log-buffer entries

default log-buffer entries

Parameter Description

number: Configured buffer size, in pieces. The value range is from 0 to 1024.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the size of the NFPP log buffer to 50 pieces.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer entries 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 log-buffer logs

Function

Run the **log-buffer logs** command to configure the rate of generating system messages from logs of the log buffer through NFPP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No rate of generating system messages from logs of the log buffer is configured through NFPP and NFPP logs are not written into the buffer by default.

Syntax

log-buffer logs *message-number* **interval** *interval*

no log-buffer logs

default log-buffer logs

Parameter Description

message-number: Number of system messages output in the specified *interval*, in pieces. The value range is from 0 to 1024. The value **0** specifies that logs are recorded in the special buffer without generating system messages.

interval: Time configured to generate *message-number* system messages, in seconds. The value range is from 0 to 86400. The value **0** specifies that logs are not written into the log buffer, but are used to immediately generate system messages.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the values of *message-number* and *interval* are 0, logs are not written into the log buffer, but are used to immediately generate system messages.

The result of *message-number* divided by *interval* specifies the rate of generating system messages from logs of the log buffer.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to 0:

- If the **log-buffer enable** command is also configured, logs are output onto the screen without limit.
- If the **log-buffer enable** command is not configured, the logs related to isolation and port rate limit are output onto the screen without limit by the **log-buffer logs** command and other types of logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to 0 and the value of *interval* to a none-zero value: Logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the values of the *message-number* and *interval* parameters to non-zero values:

- If the log-buffer enable command is configured, logs are first stored in the log buffer and then output onto the screen regularly based on the *interval* configuration.
- If the **log-buffer enable** command is not configured, logs are first stored in the log buffer, and logs related to isolation and port rate limit are output onto the screen regularly based on the *interval* configuration.

When logs are first output onto the screen, the historical logs in the log buffer are output onto the screen. Before starting the configuration, you are advised to run the **clear nfpp log** command to clear the logs in the log buffer.

Examples

The following example sets the system message generation rate to 2 logs per 12 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer logs 2 interval 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 logging

Function

Run the **logging** command to configure NFPP to records the logs of a specified VLAN ID and a specified interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

NFPP records logs of all VLANs and interfaces by default.

Syntax

logging { **interface** *interface-type interface-number* | **vlan** *vlan-range* }

no logging { **interface** *interface-type interface-number* | **vlan** *vlan-range* }

default logging

Parameter Description

interface *interface-type interface-number*: Records only the NFPP logs of a specified interface.

vlan *vlan-range*: Records only the NFPP logs in the specified VLAN range. The value range is from 1 to 4095. The input format is as follows: 1-3, 5.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

This command can be used to filter logs and record the logs of a specified VLAN range or an interface. If the relationship of two log filtering configurations is OR, logs are recorded into the log buffer when one log filtering configuration is met.

Examples

The following example records the logs of VLAN 1, VLAN 2, VLAN 3, and VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# logging vlan 1-3,5
```

The following example records the logs on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# logging interface gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 match

Function

Run the **match** command to configure the matched packet types of a customized guard type.

Syntax

match { **dst-ip** *destination-ipv4-address* [**dst-ip-mask** *mask*] | **dst-ipv6** *destination-ipv6-address* [**dst-ipv6-masklen** *prefix-length*] | **dst-mac** *destination-mac* [**dst-mac-mask** *destination-mac-mask*] | **dst-port** *port-number* | **etype** *type* | **protocol** *protocol* | **src-ip** *source-ip-address* [**src-ip-mask** *mask*] | **src-ipv6** *source-ipv6-address* [**src-ipv6-masklen** *prefix-length*] | **src-mac** *source-mac-address* | **src-port** *port-number* } *

Parameter Description

dst-ip *destination-ipv4-address*: Specifies a destination IPv4 address.

dst-ip-mask *mask*: Specifies a destination IPv4 address mask.

dst-ipv6 *destination-ipv6-address*: Specifies a destination IPv6 address.

dst-ipv6-masklen *prefix-length*: Specifies the length of a destination IPv6 address mask.

dst-mac *destination-mac*: Specifies a destination MAC address.

dst-mac-mask *destination-mac-mask*: Specifies a destination MAC address mask.

dst-port *port-number*: Specifies a destination port number on the transport layer.

etype *type*: Specifies an Ethernet link layer packet type.

protocol *protocol*: Specifies a protocol number.

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

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

src-ipv6 *source-ipv6-address*: Specifies a source IPv6 address.

src-ipv6-masklen *prefix-length*: Specifies the length of a source IPv6 address mask.

src-mac *source-mac-address*: Specifies a source MAC address.

src-port *port-number*: Specifies a source port number on the transport layer.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

After you create a customized guard type, you must specify packet fields to match this guard type.

Examples

The following example creates a customized TCP guard type and matches packets with **etype** being **0x0800** and **protocol** being **0x06**.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# match etype 0x0800 protocol 0x06
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 monitored-host-limit

Function

Run the **monitored-host-limit** command to configure the maximum number of monitored hosts of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts is **20000** by default.

Syntax

monitored-host-limit *number*

no monitored-host-limit

default monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DEFINE_GUARD -SESSION_LIMIT: Attempt to exceed limit of name (name of a customized guard type)'s 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of the customized TCP guard type to **500**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# monitored-host-limit 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 monitor-period

Function

Run the **monitor-period** command to configure the monitoring time of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of a customized guard type is **600** seconds.

Syntax

monitor-period *interval*

no monitor-period

default monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

When customized guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of the customized TCP guard type to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# monitor-period 180
```

Platform Description

N/A

Related Commands

N/A

1.57 nd-guard attack-threshold per-port

Function

Run the **nd-guard attack-threshold per-port** command to configure the global attack threshold of ND guard.

Run the **no** form of command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ND guard for NDSNP packets is 200 pps, for neighbor requests and advertisements is 100 pps, for route advertisements and redirection packets is 50 pps, and for route requests is 50 pps.

Syntax

nd-guard attack-threshold per-port { **ndsnp** *attack-threshold* | **ns-na** *attack-threshold* | **ra-redirect** *attack-threshold* | **rs** *attack-threshold* }

no nd-guard attack-threshold per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nd-guard attack-threshold per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp *attack-threshold*: Configures an attack threshold for NDSNP packets, in pps. The value range is from 1 to 19999. After the **ipv6 nd snooping enable** command is run in global configuration mode, all ND packets are NDSNP packets.

ns-na *attack-threshold*: Configures an attack threshold for neighbor requests and advertisements, in pps. The value range is from 1 to 19999.

ra-redirect *attack-threshold*: Configures an attack threshold for route advertisements and redirection packets, in pps. The value range is from 1 to 19999.

rs *attack-threshold*: Configures an attack threshold for route requests, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the global attack thresholds of ND guard to **10** pps, **20** pps, **10** pps, and **10** pps for NDSNP packets, neighbor requests and advertisements, route advertisements and redirection packets, and route requests respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard attack-threshold per-port ndsnp 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Hostname(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port rs 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 nd-guard enable

Function

Run the **nd-guard enable** command to enable the function of global ND guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ND guard is enabled by default.

Syntax

nd-guard enable

no nd-guard enable

default nd-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ND guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 nd-guard rate-limit per-port

Function

Run the **nd-guard rate-limit per-port** command to configure the global rate limiting threshold of ND guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ND guard for NDSNP packets is 100 pps, for neighbor requests and advertisements is 50 pps, for route advertisements and redirection packets is 25 pps, and for route requests is 25 pps.

Syntax

nd-guard rate-limit per-port { **ndsnp** *rate-limit* | **ns-na** *rate-limit* | **ra-redirect** *rate-limit* | **rs** *rate-limit* }

no nd-guard rate-limit per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nd-guard rate-limit per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp *rate-limit*: Configures a rate limiting threshold for NDSNP packets, in pps. The value range is from 1 to 19999. After the **ipv6 nd snooping enable** command is run in global configuration mode, all ND packets are NDSNP packets.

ns-na *rate-limit*: Configures a rate limiting threshold for neighbor requests and advertisements, in pps. The value range is from 1 to 19999.

ra-redirect *rate-limit*: Configures a rate limiting threshold for route advertisements and redirection packets, in pps. The value range is from 1 to 19999.

rs *rate-limit*: Configures a rate limiting threshold for route requests, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ND guard to **5** pps, **10** pps, **5** pps, and **5** pps for NDSNP packets, neighbor requests and advertisements, route advertisements and redirection packets, and route requests respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard rate-limit per-port ndsnp 5
Hostname(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Hostname(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
Hostname(config-nfpp)# nd-guard rate-limit per-port rs 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 nd-guard ratelimit-forwarding enable

Function

Run the **nd-guard ratelimit-forwarding enable** command to enable the function of port-based rate limit forwarding of ND guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of port-based rate limit forwarding of ND guard is enabled by default.

Syntax

nd-guard ratelimit-forwarding enable

no nd-guard ratelimit-forwarding enable

default nd-guard ratelimit-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of port-based rate limit forwarding of ND guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 nfpp

Function

Run the **nfpp** command to enter the NFPP configuration mode.

Syntax

nfpp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enter the NFPP configuration mode for NFPP configuration.

Examples

The following example enters the NFPP configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 nfpp arp-guard enable

Function

Run the **nfpp arp-guard enable** command to enable the ARP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ARP guard function is not configured on an interface by default. The function of global ARP guard is enabled.

Syntax

nfpp arp-guard enable

no nfpp arp-guard enable

default nfpp arp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ARP guard function on an interface takes precedence over the function of global ARP guard.

Examples

The following example enables the ARP guard function on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 nfpp arp-guard isolate-period

Function

Run the **nfpp arp-guard isolate-period** command to configure the isolation time of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No isolation time of ARP guard is configured on an interface by default. The global isolation time of ARP guard is used.

Syntax

nfpp arp-guard isolate-period { *interval* | **permanent** }

no nfpp arp-guard isolate-period

default nfpp arp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the isolation time of ARP guard on interface GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 nfpp arp-guard policy

Function

Run the **nfpp arp-guard policy** command to configure the local rate limiting threshold and local attack threshold of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ARP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ARP guard are used.

Syntax

nfpp arp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp arp-guard policy { **per-port** | **per-src-ip** | **per-src-mac** }

default nfpp arp-guard policy { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of ARP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1, to **2** pps and **10** pps for each source IP address, and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-src-ip 2 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-src-mac 3 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.65 nfpp arp-guard scan-threshold

Function

Run the **nfpp arp-guard scan-threshold** command to configure the scanning threshold of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No scanning threshold of ARP guard is configured on an interface by default. The global scanning threshold of ARP guard is used.

Syntax

nfpp arp-guard scan-threshold *scan-threshold*

no nfpp arp-guard scan-threshold

default nfpp arp-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the scanning threshold of ARP guard on GigabitEthernet 0/1 to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 nfpp define enable

Function

Run the **nfpp define enable** command to enable the customized guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The customized guard function is not configured on an interface by default. The global customized guard function is used.

Syntax

nfpp define *define-name* **enable**

no nfpp define *define-name* **enable**

default nfpp define *define-name* **enable**

Parameter Description

define-name: Name of a customized guard type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

A customized guard type must be configured. To validate this configuration, you must configure the **match** and **global-policy** parameters.

Examples

The following example enables the function of customized TCP guard on GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.67 nfpp define policy

Function

Run the **nfpp define policy** command to configure a local rate limiting threshold and a local attack threshold of customized guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of the customized guard type is configured on an interface by default. The global rate limiting threshold and global attack threshold of the customized guard type are used.

Syntax

nfpp define *define-name* **policy** { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp define *define-name* **policy** { **per-port** | **per-src-ip** | **per-src-mac** }

default nfpp define *define-name* **policy** { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

define *define-name*: Name of a specified customized guard type.

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of the customized TCP guard function to **2** pps and **10** pps on GigabitEthernet 0/1 for an IP address, and to **50** pps and **100** pps for an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp policy per-src-ip 2 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp policy per-port 50 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 nfpp dhcp-guard enable

Function

Run the **nfpp dhcp-guard enable** command to enable the DHCP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCP guard function is not configured on an interface by default. The function of global DHCP guard is used.

Syntax

nfpp dhcp-guard enable

no nfpp dhcp-guard enable

default nfpp dhcp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The DHCP guard function on an interface takes precedence over the global DHCP guard function.

Examples

The following example enables the DHCP guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.69 nfpp dhcp-guard isolate-period

Function

Run the **nfpp dhcp-guard isolate-period** command to configure the local isolation time of DHCP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of DHCP guard is configured on an interface by default. The global isolation time of DHCP guard is used.

Syntax

nfpp dhcp-guard isolate-period { *interval* | **permanent** }

no nfpp dhcp-guard isolate-period

default nfpp dhcp-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of DHCP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.70 nfpp dhcp-guard policy

Function

Run the **nfpp dhcp-guard policy** command to configure a local rate limiting threshold and a local attack threshold of DHCP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of DHCP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCP guard are used.

Syntax

nfpp dhcp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp dhcp-guard policy { **per-port** | **per-src-mac** }

default nfpp dhcp-guard policy { **per-port** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of DHCP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard policy per-src-mac 3 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.71 nfpp dhcpv6-guard enable

Function

Run the **nfpp dhcpv6-guard enable** command to enable the DHCPv6 guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCPv6 guard function is disabled on an interface by default. The global DHCPv6 guard function is used.

Syntax

nfpp dhcpv6-guard enable

no nfpp dhcpv6-guard enable

default nfpp dhcpv6-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The DHCPv6 guard function on an interface takes precedence over the global DHCP guard function.

Examples

The following example enables the DHCPv6 guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcpv6-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.72 nfpp dhcpv6-guard policy

Function

Run the **nfpp dhcpv6-guard policy** command to configure a local rate limiting threshold and a local attack threshold of DHCPv6 guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of DHCPv6 guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCPv6 guard are used.

Syntax

nfpp dhcpv6-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp dhcpv6-guard policy { **per-port** | **per-src-mac** }

default nfpp dhcpv6-guard policy { **per-port** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of DHCPv6 guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcpv6-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcpv6-guard policy per-src-mac 3 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.73 nfpp icmp-guard enable

Function

Run the **nfpp icmp-guard enable** command to enable the ICMP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ICMP guard function is not configured on an interface by default. The function of global ICMP guard is used.

Syntax

nfpp icmp-guard enable

no nfpp icmp-guard enable

default nfpp icmp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ICMP guard function on an interface takes precedence over the function of global ICMP guard.

Examples

The following example enables the ICMP guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.74 nfpp icmp-guard isolate-period

Function

Run the **nfpp icmp-guard isolate-period** command to configure the local isolation time of ICMP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of ICMP guard is configured on an interface by default. The global isolation time of ICMP guard is used.

Syntax

nfpp icmp-guard isolate-period { *interval* | **permanent** }

no nfpp icmp-guard isolate-period

default nfpp icmp-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of ICMP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.75 nfpp icmp-guard policy

Function

Run the **nfpp icmp-guard policy** command to configure a local rate limiting threshold and a local attack threshold of ICMP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ICMP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ICMP guard are used.

Syntax

nfpp icmp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp icmp-guard policy { **per-port** | **per-src-ip** }

default nfpp icmp-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of ICMP guard to **100** pps and **200** pps for each interface on GigabitEthernet 0/1 and to **5** pps and **10** pps for each source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard policy per-port 100 200
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard policy per-src-ip 5 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.76 nfpp ip-guard enable

Function

Run the **nfpp ip-guard enable** command to enable the IP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No IP guard function is configured on an interface by default. The global IP guard function is enabled.

Syntax

nfpp ip-guard enable

no nfpp ip-guard enable

default nfpp ip-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The IP guard function on an interface takes precedence over the function of global IP guard.

If the function of ARP source suppression is enabled and the isolation time is configured for the IP guard function in global or interface configuration mode, an error is reported when you enable the IP guard function.

Examples

The following example enables the IP guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard enable
```

Notifications

No notification can be configured.

```
Configuration is prohibited, please disable the arp-guard suppression function first!
```

Common Errors

If the function of ARP source suppression is configured on an interface and the isolation time is configured for the IP guard function in global or interface configuration mode, an error is reported when you configure the IP guard function on this interface.

Platform Description

N/A

Related Commands

N/A

1.77 nfpp ip-guard isolate-period

Function

Run the **nfpp ip-guard isolate-period** command to configure the local isolation time of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No isolation time of IP guard is configured by default. The global isolation time of IP guard is used.

Syntax

nfpp ip-guard isolate-period { *interval* | **permanent** }

no nfpp ip-guard isolate-period

default nfpp ip-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If you have configured the function of ARP source suppression, you cannot configure the isolation time for the IP guard function.

Examples

The following example sets the local isolation time of IP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard isolate-period 180
```

Notifications

If you have configured the function of ARP source suppression, the following notification will be displayed when you configure isolation time for IP guard:

```
Configuration is prohibited, please disable the arp-guard suppression function first!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.78 nfpp ip-guard policy

Function

Run the **nfpp ip-guard policy** command to configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of IP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of IP guard are used.

Syntax

nfpp ip-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp ip-guard policy { **per-port** | **per-src-ip** }

default nfpp ip-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of IP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **2** pps and **10** pps for each source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard policy per-src-ip 2 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.79 nfpp ip-guard scan-threshold

Function

Run the **nfpp ip-guard scan-threshold** command to configure the local scanning threshold of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No scanning threshold of IP guard is configured on an interface by default. The global scanning threshold of IP guard is used.

Syntax

nfpp ip-guard scan-threshold *scan-threshold*

no nfpp ip-guard scan-threshold

default nfpp ip-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the scanning threshold of IP guard on GigabitEthernet 0/1 to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.80 nfpp nd-guard enable

Function

Run the **nfpp nd-guard enable** command to enable the ND guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ND guard function is not configured on an interface by default. The function of global ND guard is used.

Syntax

nfpp nd-guard enable

no nfpp nd-guard enable

default nfpp nd-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ND guard function on an interface takes precedence over the global ND guard function.

Examples

The following example enables the ND guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.81 nfpp nd-guard policy per-port

Function

Run the **nfpp nd-guard policy per-port** command to configure a local rate limiting threshold and a local attack threshold of ND guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ND guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ND guard are used.

Syntax

nfpp nd-guard policy per-port { **ndsnp** *rate-limit attack-threshold* | **ns-na** *rate-limit attack-threshold* | **ra-redirect** *rate-limit attack-threshold* | **rs** *rate-limit attack-threshold* }

no nfpp nd-guard policy per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nfpp nd-guard policy per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp: Configures a rate limiting threshold and an attack threshold for NDSNP packets. After the **ipv6 nd snooping enable** command is enabled in global configuration mode, all ND packets are NDSNP packets.

ns-na: Configures a rate limiting threshold and an attack threshold for neighbor requests and advertisements.

ra-redirect: Configures a rate limiting threshold and an attack threshold for route advertisements and redirection packets.

rs: Configures a rate limiting threshold and an attack threshold for route requests.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of ND guard to **5** pps and **10** pps for NDSNP packets on interface GigabitEthernet 0/1, to **50** pps and **100** pps for neighbor requests and advertisements, to **10** pps and **20** pps for route advertisements and redirection packets, and to **10** pps and **20** pps for route requests.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ndsnp 5 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ns-na 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ra-redirect
10 20
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port rs 10 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.82 nfpp tcp-syn-guard enable

Function

Run the **nfpp tcp-syn-guard enable** command to enable the TCP-SYN guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The TCP-SYN guard function is not configured on an interface by default. The function of global TCP-SYN function is used.

Syntax

nfpp tcp-syn-guard enable

no nfpp tcp-syn-guard enable

default nfpp tcp-syn-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The TCP-SYN guard function on an interface takes precedence over the global TCP-SYN guard function.

Examples

The following example enables the TCP-SYN guard function on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.83 nfpp tcp-syn-guard isolate-period

Function

Run the **nfpp tcp-syn-guard isolate-period** command to configure the local isolation time of TCP-SYN guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of TCP-SYN guard is configured by default. The global isolation time of TCP-SYN guard is used.

Syntax

nfpp tcp-syn-guard isolate-period { *interval* | **permanent** }

no nfpp tcp-syn-guard isolate-period

default nfpp tcp-syn-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of TCP-SYN guard on interface GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.84 nfpp tcp-syn-guard policy

Function

Run the **nfpp tcp-syn-guard policy** command to configure a local rate limiting threshold and a local attack threshold of TCP-SYN guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of TCP-SYN guard is configured on an interface by default. The global rate limiting threshold and attack threshold of TCP-SYN guard are used.

Syntax

nfpp tcp-syn-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp tcp-syn-guard policy { **per-port** | **per-src-ip** }

default nfpp tcp-syn-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of TCP-SYN guard to **50** pps and **100** pps for each interface on interface GigabitEthernet 0/1 and to **2** pps and **10** pps for each source IP address.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard policy per-src-ip 2 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.85 show nfpp arp-guard hosts

Function

Run the **show nfpp arp-guard hosts** command to display the monitored hosts of ARP guard.

Syntax

show nfpp arp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed. Whether this parameter is supported depends on the actual product version.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ARP guard.

```
Hostname> enable
```

```
Hostname# show nfpp arp-guard hosts statistics
success    fail    total
---    --    -------
100      20     120
```

Table 1-1 Output Field of the show nfpp arp-guard hosts statistics Command

Field	Description
Success	Number of isolated hosts
Fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ARP guard.

```
Hostname# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address     remain-time(s)
--  ----   ---    -----     -----
1     Gi0/1      1.1.1.1     -               110
2     Gi0/2      1.1.2.1     -               61
*3    Gi0/3      -           0000.0000.1111  110
4     Gi0/4      -           0000.0000.2222   61
Total: 4 hosts
```

Table 1-2 Output Field of the show nfpp arp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.86 show nfpp arp-guard scan

Function

Run the **show nfpp arp-guard scan** command to display the scanning table of ARP guard.

Syntax

show nfpp arp-guard scan [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the scanning table.

vlan *vlan-id*: Displays the scanning table of a specified VLAN ID.

interface *interface-type interface-number*: Displays the scanning table of a specified interface.

mac-address: Specified MAC address of a scanning table.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the scanning table of ARP guard.

```
Hostname> enable
Hostname# show nfpp arp-guard scan statistics
arp-guard scan table has 4 record(s).
```

Table 1-3 Output Field of the show nfpp arp-guard scan statistics Command

Field	Description
arp-guard scan table has *number* record(s).	Displays the number of records in the scanning table. *number* specifies the number of records in the scanning table.

The following example displays the scanning table of ARP guard. "timestamp" specifies the detection time of ARP scanning. For example, "2008-01-23 16:23:10" specifies that ARP scanning time is detected at 16:23:10 on January 23, 2008.

```
Hostname> enable
Hostname# show nfpp arp-guard scan
```

```
VLAN   interface   IP address   MAC address     timestamp
--   ----   ----  -----     ---
1       Gi0/1      -         0000.0000.0001   2008-01-23 16:23:10
2       Gi0/2      1.1.1.1     0000.0000.0002   2008-01-23 16:24:10
3       Gi0/3      -         0000.0000.0003   2008-01-23 16:25:10
4       Gi0/4      -         0000.0000.0004   2008-01-23 16:26:10
Total: 4 record(s)
```

Table 1-4 Output Field of the show nfpp arp-guard hosts Command

Field	Description
VLAN	VLAN ID of the ARP scanning information
interface	Interface name of the ARP scanning information
IP address	IP address of the ARP scanning information
MAC address	MAC address of the ARP scanning information
timestamp	Detection time of the ARP scanning
Total: *number* record(s)	Total number of records in the ARP scanning table. *number* specifies the specific number of records in the scanning table.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.87 show nfpp arp-guard summary

Function

Run the **show nfpp arp-guard summary** command to display the configuration information of ARP guard.

Syntax

show nfpp arp-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ARP guard.

```
Hostname> enable
Hostname# show nfpp arp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global     Enable  300            4/5/60    8/10/100         15
Gi 0/1      Enable  180            5/-      8/-             -
Gi 0/2      Disable 200            4/5/60    8/10/100         20
Maximum count of monitored hosts: 1000
Monitor period: 300s
Suppress-mode: disable
Suppress-threshold: 5pps
Suppress-period: 5s
```

Table 1-5 Output Field of the show nfpp arp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolat-period	Isolation period configured in a policy, in seconds
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Scan-threshold	Scanning threshold
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds
suppress-mode	Whether the suppression mode is enabled: ● **Enable**: The mode is enabled.

Field	Description
	● **Disable**: The mode is disabled.
suppress-threshold	Suppression threshold, in pps
suppress-period	Suppression period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.88 show nfpp define hosts

Function

Run the **show nfpp define hosts** command to display the monitored hosts of a customized guard type.

Syntax

show nfpp define hosts *name* [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address* | *ipv6-address*]]

Parameter Description

name: Name of a specified customized guard type.

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

mac-address: Specified MAC address of a monitored host.

ipv6-address: Specified IPv6 address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Parameters can be configured in the command to filter unwanted monitored hosts.

Examples

The following example displays the monitored hosts of a customized TCP guard type.

```
Hostname> enable
Hostname# show nfpp define hosts tcp
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   MAC address    remain-time(s)
 --    ---   -----     ------
*1      Gi4/2      00d0.f822.33e5  592
Total: 1 host
```

Table 1-6 Output Field of the show nfpp define hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time of a host, in seconds
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.89 show nfpp define summary

Function

Run the **show nfpp define summary** command to display the configuration information of a customized summary type.

Syntax

show nfpp define summary [*name*]

Parameter Description

name: Name of a specified customized guard type.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of the customized TCP guard type.

```
Hostname> enable
Hostname# show nfpp define summary abc
Define abc summary:
match etype 0x800 src-ip 1.1.1.1 src-ip-mask 255.255.255.255
Maximum count of monitored hosts: 20000
Monitor period:600s
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status  Rate-limit     Attack-threshold
Global    Disable -/10/-         -/20/-
Gi4/1     Enable  -/-          -/-/-
```

Table 1-7 Output Field of the show nfpp define summary Command

Field	Description
Define *name* summary	Configuration of a specified customized guard type. *name* specifies the name of a customized guard type.
match etype *etype* src-ip *source-ipv4-address* src-ip-mask *source-mask*	Matched packet types of a customized guard type
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring time, in seconds
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.90 show nfpp define trusted-host

Function

Run the **show nfpp define trusted-host** command to display the trusted hosts of a customized guard type.

Syntax

show nfpp define trusted-host *name*

Parameter Description

name: Name of a customized guard type.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of the customized TCP guard type.

```
Hostname> enable
Hostname# show nfpp define trusted-host tcp
Define tcp:
IP address     mask
---      -
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total: 2 record(s)
```

Table 1-8 Output Field of the show nfpp define trusted-host Command

Field	Description
Define *name*	Information of a specified customized guard type. *name* specifies the name of a customized guard type.
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host

Field	Description
Total: *number* record(s)	Total number of trusted hosts. *number* -specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.91 show nfpp dhcp-guard hosts

Function

Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts of DHCP guard.

Syntax

show nfpp dhcp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of DHCP guard.

```
Hostname> enable
Hostname# show nfpp dhcp-guard hosts statistics
success   fail   total
---   --   --
100       20      120
```

Table 1-9 Output Field of the show nfpp dhcp-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
Fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of DHCP guard.

```
Hostname> enable
Hostname# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address    remain-time(seconds)
--    ---    -----        ------
 1    gi0/2     0000.0000.0001   10
 *2   gi0/1     0000.0000.0002   20
Total: 2 host(s)
```

Table 1-10 Output Field of the show nfpp dhcp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.92 show nfpp dhcp-guard summary

Function

Run the **show nfpp dhcp-guard summary** command to display the configuration information of DHCP guard.

Syntax

show nfpp dhcp-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of DHCP guard.

```
Hostname> enable
Hostname# show nfpp dhcp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
Gi 0/1      Enable  180            -/6/-      -/8/-
Gi 0/2      Disable 200            -/5/30     -/10/50
Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Table 1-11 Output Field of the show nfpp dhcp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively

Field	Description
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.93 show nfpp dhcpv6-guard hosts

Function

Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts of DHCPv6 guard.

Syntax

show nfpp dhcpv6-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the monitored hosts of DHCPv6 guard.

```
Hostname> enable
```

```
Hostname# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address    remain-time(seconds)
--    ---    -----        -------
 *1    gi0/2     0000.0000.0001   10
 *2   gi0/1     0000.0000.0002   20
Total: 2 host(s)
```

Table 1-12 Output Field of the show nfpp dhcpv6-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
MAC address	MAC address of a host
remain-time(seconds)	Remaining isolation time for a host
Total	Maximum number of monitored hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.94 show nfpp dhcpv6-guard summary

Function

Run the **show nfpp dhcpv6-guard summary** command to display the configuration information of DHCPv6 guard.

Syntax

show nfpp dhcpv6-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of DHCPv6 guard.

```
Hostname> enable
Hostname# show nfpp dhcpv6-guard summary
 (Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status  Rate-limit     Attack-threshold
Global    Enable  -/5/1200       -/10/1500
Maximum count of monitored hosts: 20000
Monitor period: 600s
```

Table 1-13 Output Field of the show nfpp dhcpv6-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.95 show nfpp icmp-guard hosts

Function

Run the **show nfpp icmp-guard hosts** command to display the monitored hosts of ICMP guard.

Syntax

show nfpp icmp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ICMP guard.

```
Hostname> enable
Hostname# show nfpp icmp-guard hosts statistics
success    fail    total
---    --    ---
100        20       120
```

Table 1-14 Output Field of the show nfpp icmp-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ICMP guard.

```
Hostname> enable
Hostname# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
```

```
--    ----   ---          -----
1     Gi0/1      1.1.1.1     110
2     Gi0/2      1.1.2.1     61
Total: 2 host(s)
```

Table 1-15 Output Field of the show nfpp icmp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.96 show nfpp icmp-guard summary

Function

Run the **show nfpp icmp-guard summary** command to display the configuration information of ICMP guard.

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ICMP guard.

```
Hostname> enable
Hostname# show nfpp icmp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            4/-/60    8/-/100
Gi 0/1      Enable  180            5/-      8/-/-
Gi 0/2      Disable 200            4/-/60    8/-/100
Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Table 1-16 Output Field of the show nfpp icmp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.97 show nfpp icmp-guard trusted-host

Function

Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts of ICMP guard.

Syntax

show nfpp icmp-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the monitored trusted hosts of ICMP guard.

```
Hostname> enable
Hostname# show nfpp icmp-guard trusted-host
IP address     mask
---      --
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total: 2 record(s)
```

Table 1-17 Output Field of the show nfpp icmp-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.98 show nfpp ip-guard hosts

Function

Run the **show nfpp ip-guard hosts** command to display the monitored hosts of IP guard.

Syntax

show nfpp ip-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of IP guard.

```
Hostname> enable
Hostname# show nfpp ip-guard hosts statistics
success    fail    total
---    --    ---
100        20       120
```

Table 1-18 Output Field of the show nfpp ip-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of IP guard.

```
Hostname> enable
Hostname# show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address   Reason     remain-time(s)
--  ----   ---   ---     -----
1     Gi0/1      1.1.1.1     ATTACK     110
2     Gi0/2      1.1.2.1     SCAN        61
Total: 2 host(s)
```

Table 1-19 Output Field of the show nfpp ip-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
Reason	Reason of host monitoring: ● **ATTACK**: Specifies that IP packets are sent at a rate higher than the attack threshold. ● **SCAN**: Specifies that a host is scanning a network segment.
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.99 show nfpp ip-guard summary

Function

Run the **show nfpp ip-guard summary** command to display the configuration information of IP guard.

Syntax

show nfpp ip-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of IP guard.

```
Hostname> enable
Hostname# show nfpp ip-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global     Enable  300            4/-/60    8/-/100         15
Gi 0/1      Enable  180            5/-/-      8/-/-            -
Gi 0/2      Disable 200            4/-/60    8/-/100          20
Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Table 1-20 Output Field of the show nfpp ip-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Scan-threshold	Scanning threshold
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.100 show nfpp ip-guard trusted-host

Function

Run the **show nfpp ip-guard trusted-host** command to display the trusted hosts of IP guard.

Syntax

show nfpp ip-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of IP guard.

```
Hostname> enable
Hostname# show nfpp ip-guard trusted-host
IP address     mask
---      --
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total: 2 record(s)
```

Table 1-21 Output Field of the show nfpp ip-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host

Field	Description
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.101 show nfpp log buffer

Function

Run the **show nfpp log buffer** command to display the information in the log buffer of NFPP.

Syntax

show nfpp log buffer

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the log buffer overflows, subsequent logs are discarded, and the log buffer displays an entry with attributes being "-". In this case, the administrator must increase the log buffer size or improve the generation rate of system messages.

The system message generated from logs of the log buffer carries the event timestamp, as shown below:

```
%NFPP_ARP_GUARD-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>
was detected.(2009-07-01 13:00:00)
```

Examples

The following example displays the log buffer of NFPP.

```
Hostname> enable
Hostname# show nfpp log buffer
Protocol VLAN  Interface IP address MAC address    Reason        Timestamp
---- ----   --- -----    --         ---
```

```
ARP    1     Gi0/1     1.1.1.1     -           DoS            2009-05-30
16:23:10
ARP    1     Gi0/1     1.1.1.1     -           ISOLATED       2009-05-30
16:23:10
ARP    1     Gi0/1     1.1.1.2     -           DoS            2009-05-30
16:23:15
ARP    1     Gi0/1     1.1.1.2     -           ISOLATE_FAILED 2009-05-30 16:23:15
ARP    1     Gi0/1     -        0000.0000.0001  SCAN           2009-05-30
16:30:10
ARP    -     Gi0/2     -        -              PORT_ATTACKED   2009-05-30
16:30:10
ND-SNP 258   Te0/1     -        -              PORT_ATTACKED   2019-28 9:31:39
```

Table 1-22 Output Field of the show nfpp log buffer Command

Field	Description
Protocol	Corresponding packet protocol
VLAN	VLAN ID
Interface	Corresponding interface
IP address	Corresponding IP address
MAC address	Corresponding MAC address
Reason	Reason for recording
Timestamp	Timestamp of recording

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.102 show nfpp log buffer statistics

Function

Run the **show nfpp log buffer statistics** command to display the statistics about the log buffer of NFPP.

Syntax

show nfpp log buffer statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the log buffer of NFPP.

```
Hostname# show nfpp log buffer statistics
There are 6 logs in buffer.
```

Table 1-23 Output Field of the show nfpp log buffer statistics Command

Field	Description
There are *number* logs in buffer.	Number of logs in the log buffer. *number* specifies the specific number.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.103 show nfpp log summary

Function

Run the **show nfpp log summary** command to display the configuration information of NFPP logs.

Syntax

show nfpp log summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of NFPP logs.

```
Hostname> enable
Hostname# show nfpp log summary
Total log buffer size:10
Syslog rate: 1 entry per 2 seconds
Logging:
VLAN 1-3, 5
interface Gi 0/1
interface Gi 0/2
```

Table 1-24 Output Field of the show nfpp log summary Command

Field	Description
Total log buffer size	Buffer size
Syslog rate	Log print rate
Logging	Recorded VLAN and interface information

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.104 show nfpp nd-guard hosts

Function

Run the **show nfpp nd-guard hosts** command to display the monitored hosts of ND guard.

Syntax

show nfpp nd-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ND guard.

```
Hostname> enable
Hostname# show nfpp nd-guard hosts statistics
success    fail    total
---    --    --
10        2       12
```

Table 1-25 Output Field of the show nfpp nd-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ND guard.

```
Hostname> enable
Hostname# show nfpp nd-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   ND-guard          remain-time(s)
 --    ---   ----          ------
 -      Gi4/2      ns-na-guard        174
 -      Gi4/2      rs-guard          98
 -      Gi4/2      ra-redirect-guard   127
Total: 3 hosts
```

Table 1-26 Output Field of the show nfpp nd-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host

Field	Description
ND-guard	Packet type of ND guard
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.105 show nfpp nd-guard summary

Function

Run the **show nfpp nd-guard summary** command to display the configuration information of ND guard.

Syntax

show nfpp nd-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ND guard, including global configuration information and configuration information on an interface.

```
Hostname> enable
Hostname# show nfpp nd-guard summary
(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT/ND-SNP.)
Interface  Status  Rate-limit Attack-threshold
Global     Enable  20/5/10/25    40/10/20/50
```

```
Gi 0/1      Enable  15/15/15/25   30/30/30/50
Gi 0/2      Disable -/5/30/25      -/10/50/50
```

Table 1-27 Output Field of the show nfpp nd-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for neighbor requests and advertisements, route requests, route advertisement and redirection packets, and NDSNP packets respectively
Attack-threshold	Attack thresholds for neighbor requests and advertisements, route requests, route advertisement and redirection packets, and NDSNP packets respectively

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.106 show nfpp tcp-syn-guard hosts

Function

Run the **show nfpp tcp-syn-guard hosts** command to display the monitored hosts of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-guard hosts statistics
success    fail    total
---    --    ---
100        20       120
```

Table 1-28 Output Field of the show nfpp tcp-syn-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address   Reason     remain-time(s)
--  ----   ---   ---     -----
1     Gi0/1      1.1.1.1     ATTACK     110
2     Gi0/2      1.1.2.1     SCAN        61
Total: 2 host(s)
```

Table 1-29 Output Field of the show nfpp tcp-syn-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
Reason	Reason for host monitoring: ● **ATTACK**: Specifies that TCP-SYN packets are sent at a rate higher than the attack threshold. ● **SCAN**: Specifies that a host is scanning a network segment.

Field	Description
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.107 show nfpp tcp-syn-guard summary

Function

Run the **show nfpp tcp-syn-guard summary** command to display the configuration information of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global     Enable  300            4/-/60    8/-/100
```

```
Gi 0/1      Enable  180           5/-/-      8/-/-
Gi 0/2      Disable 200           4/-/60     8/-/100
Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Table 1-30 Output Field of the show nfpp tcp-syn-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.108 show nfpp tcp-syn-guard trusted-host

Function

Run the **show nfpp tcp-syn-guard trusted-host** command to display the trusted hosts of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-guard trusted-host
IP address     mask
---      --
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total: 2 record(s)
```

Table 1-31 Output Field of the show nfpp tcp-syn-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.109 tcp-syn-guard attack-threshold

Function

Run the **tcp-syn-guard attack-threshold** command to configure the global attack threshold of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global attack threshold of TCP-SYN guard for each interface is 200 pps and for each source IP address is 100 pps by default.

Syntax

tcp-syn-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no tcp-syn-guard attack-threshold { **per-port** | **per-src-ip** }

default tcp-syn-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.
TCP-SYN guard is to solve TCP-SYN attacks on the destination IP address, but not the local IP address. If the destination IP address is a local IP address, the rates of IP packets are limited by the function of CPU protect policy (CPP).

Examples

The following example sets the global attack thresholds of TCP-SYN guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard attack-threshold per-port 50
Hostname(config-nfpp)# tcp-syn-guard attack-threshold per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.110 tcp-syn-guard enable

Function

Run the **tcp-syn-guard enable** command to enable the global TCP-SYN guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The global TCP-SYN guard function is enabled by default.

Syntax

tcp-syn-guard enable

no tcp-syn-guard enable

default tcp-syn-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global TCP-SYN guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.111 tcp-syn-guard isolate-period

Function

Run the **tcp-syn-guard isolate-period** command to configure the global isolation time of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of TCP-SYN guard is **0**.

Syntax

tcp-syn-guard isolate-period { *interval* | **permanent** }

no tcp-syn-guard isolate-period

default tcp-syn-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global isolation time of TCP-SYN guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.112 tcp-syn-guard monitored-host-limit

Function

Run the **tcp-syn-guard monitored-host-limit** command to configure the maximum number of monitored hosts of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of TCP-SYN guard is **20000** by default.

Syntax

tcp-syn-guard monitored-host-limit *number*

no tcp-syn-guard monitored-host-limit

default tcp-syn-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to delete clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_TCP_SYN_GUARD-SESSION_LIMIT: Attempt to exceed limit of IP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of TCP-SYN guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.113 tcp-syn-guard monitor-period

Function

Run the **tcp-syn-guard monitor-period** command to configure the monitoring time of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of TCP-SYN guard is **600** seconds.

Syntax

tcp-syn-guard monitor-period *interval*

no tcp-syn-guard monitor-period

default tcp-syn-guard monitor-perio

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When TCP-SYN guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of TCP-SYN guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.114 tcp-syn-guard rate-limit

Function

Run the **tcp-syn-guard rate-limit** command to configure the global rate limiting threshold of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of TCP-SYN guard for each interface is 50 pps and for each source IP address is 20 pps.

Syntax

tcp-syn-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no tcp-syn-guard rate-limit { **per-port** | **per-src-ip** }

default tcp-syn-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of TCP-SYN guard to **40** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# tcp-syn-guard rate-limit per-port 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.115 tcp-syn-guard trusted-host

Function

Run the **tcp-syn-guard trusted-host** command to configure the trusted hosts of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of TCP-SYN guard by default.

Syntax

tcp-syn-guard trusted-host *ipv4-address mask*

no tcp-syn-guard trusted-host { *ipv4-address mask* | **all** }

default tcp-syn-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, IP packets sent by this host can be forwarded to the CPU without rate limit or alarm.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.116 trusted-host

Function

Run the **trusted-host** command to configure trusted hosts of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of the customized guard type by default.

Syntax

trusted-host { *ipv4-address mask* | *ipv6-address*/*prefix-length* | *mac-address mask* }

no trusted-host { *ipv4-address mask* | *ipv6-address*/*prefix-length* | *mac-address mask* | **all** }

default trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

ipv6-address/*prefix-length*: IPv6 address+prefix. The prefix starts with a slash (/).

Mac-address mask: MAC address and mask.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, ICMP packets sent by this host can be forwarded to the CPU without rate limit or alarm. All hosts in a network segment can be configured as trusted hosts by configuring a mask.

A maximum of 500 trusted hosts can be configured.

The match type must be configured prior to the configuration of trusted hosts. If the matched packet type is IPv4, IPv6 addresses cannot be configured as trusted. If the matched packet type is IPv6, IPv4 addresses cannot be configured as trusted.

Examples

The following example configures the host 1.1.1.1 as a trusted host of the customized guard type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# trusted-host 1.1.1.1 255.255.255.255
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A

1 Storm Control Commands

Command	Function
show storm-control	Display storm control information.
storm-control	Enable packet storm control.

1.1 show storm-control

Function

Run the **show storm-control** command to display storm control information.

Syntax

show storm-control [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface whose storm control information is displayed. If this parameter is not specified, storm control information of all interfaces is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays storm control information of GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show storm-control GigabitEthernet 0/1
Interface              Broadcast Control Multicast Control Unicast Control Action
------------------------ ----------------- ----------------- ---------------
--------
     GigabitEthernet 0/1       6400   pps       6400   pps     6400   pps    none
```

Table 1-1 Output Fields of the show storm-control Command

Field	Description
Interface	Interface name
Broadcast Control	Storm control settings for broadcast packets
Multicast Control	Storm control settings for multicast packets
Unicast Control	Storm control settings for unicast packets
Action	Action

Notifications

N/A

Platform Description

N/A

Related Commands

- **storm-control**

1.2 storm-control

Function

Run the **storm-control** command to enable packet storm control.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Packet storm control is disabled by default.

Syntax

storm-control { **broadcast** | **multicast** | **unicast** } [**level** *percent* | **pps** *packets* | *rate*]

no storm-control { **broadcast** | **multicast** | **unicast** }

default storm-control { **broadcast** | **multicast** | **unicast** }

Parameter Description

broadcast: Enables storm control for broadcast packets.

multicast: Enables storm control for multicast packets.

unicast: Enables storm control for unicast packets.

level *percent*: Configures the allowed bandwidth percentage. The value range is from 1 to 100.

pps *packets*: Configures the allowed packet rate, in packets per second. The value range is from 2 to 1488095.

rate: Configures the allowed rate, in Kbit/s. The value range is from 64 to 1000000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When excessive broadcast, multicast, or unknown unicast packets are received through a port, a data packet storm occurs, which slows down the network speed and increases the timeout probability of packet transmission. A storm may occur when topology protocol execution or network configuration is incorrect.

Storm control can be implemented to limit broadcast, multicast, or unknown unicast data flows. When receiving excessive broadcast, multicast, or unknown unicast packets, a device will temporarily forbid forwarding of packets of the same type until the data flows become normal.

Examples

The following example enables storm control for multicast packets on GigabitEthernet 0/1 and sets the allowed rate to 4 Mbit/s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# storm-control multicast 4096
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 uRPF Commands

Command	Function
clear ip urpf	Clear IPv4 Unicast Reverse Path Forwarding (uRPF) packet loss statistics.
ip verify unicast source reachable-via (Global configuration mode)	Enable IPv4 uRPF.
ip verify unicast source reachable-via (Interface configuration mode)	Enable uRPF on an interface.
ip verify urpf drop-rate compute interval	Configure the interval for calculating the uRPF IPv4/IPv6 packet loss rate.
ip verify urpf drop-rate notify	Enable uPRF packet loss information monitoring.
ip verify urpf drop-rate notify hold-down	Configure the alarm interval of the uRPF IPv4/IPv6 packet loss rate.
ip verify urpf notification threshold	Configure the threshold of the uRPF packet loss rate.
show ip urpf	Display the IPv4 uRPF configurations and statistics.

1.1 clear ip urpf

Function

Run the **clear ip urpf** command to clear IPv4 Unicast Reverse Path Forwarding (uRPF) packet loss statistics.

Syntax

clear ip urpf [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-name interface-number*: Specifies the interface whose statistics are cleared. If this parameter is not specified, statistics of all interfaces are cleared.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example clears IPv4 uRPF packet loss statistics on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ip urpf interface gigabitethernet0/1
```

The following example clears IPv4 uRPF packet loss statistics on all interfaces.

```
Hostname> enable
Hostname# clear ip urpf
```

Notifications

When IPv4 uRPF is not enabled on the specified interface, the following notification will be displayed:

```
% Interface GigabitEthernet 0/1 does not enable URPF function.
```

When no interface is specified and IPv4 uRPF is not enabled on the device, the following notification will be displayed:

```
% Device does not enable URPF function.
```

Platform Description

N/A

1.2 ip verify unicast source reachable-via (Global configuration mode)

Function

Run the **ip verify unicast source reachable-via** command to enable IPv4 uRPF.

Run the **no** form of this command to disable this feature.

IPv4 uRPF is disabled by default.

Syntax

ip verify unicast source reachable-via rx

no ip verify unicast

Parameter Description

rx: Configures the strict mode to perform a uRPF check. The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address of a received IP packet must match the inbound interface of the packet.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Based on the source address of a received IP packet, uRPF checks whether any route to the source address exists in the forwarding table and accordingly determines whether the packet is valid. If no forwarding entry is matched, the packet is determined as invalid.

You can enable uRPF in global configuration mode to perform a uRPF check for packets received on all interfaces of a device.

Only the uRPF strict mode can be configured in global configuration mode. If a matched equal-cost route is found for a packet, the packet will be processed according to the uRPF loose mode.

If uRPF is configured in global configuration mode, the default route cannot be used for a uRPF check.

uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

Examples

The following example enables IPv4 uRPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify unicast source reachable-via rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip verify unicast source reachable-via (Interface configuration mode)

Function

Run the **ip verify unicast source reachable-via** command to enable uRPF on an interface.

Run the **no** form of this command to disable this feature.

uRPF is disabled for an interface by default.

Syntax

ip verify unicast source reachable-via { **any** | **rx** } [**allow-default**]

no ip verify unicast

Parameter Description

any: Configures the loose mode to perform a uRPF check. The loose mode only requires that a forwarding entry can be found in the forwarding table based on the source address of a received IP packet.

rx: Configures the strict mode to perform a uRPF check. The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address of a received IP packet must match the inbound interface of the packet.

allow-default: Allows to use the default route for a uRPF check. If this parameter is not specified, the default route is not used for a uPRF check.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, a switch will perform a uRPF check on both IPv4 and IPv6 packets.

A switch supports configuration of uRPF on a routed port, a L3 aggregation port (AP) or a switch virtual interface (SVI).

Based on the source address of a received IP packet, uRPF checks whether any route to the source address exists in the forwarding table and accordingly determines whether the packet is valid. If no forwarding entry is matched, the packet is determined as invalid.

You can enable uRPF in interface configuration mode to perform a uRPF check for packets received on the interface.

The default route is not used for a uRPF check by default. You can use the **allow-default** keyword to use the default route for a URPF check if necessary.

- uRPF does not support association with the ACL option.
- uRPF does not support the use of IPv6 routes with a 65-bit to 127-bit prefix for a uRPF check.
- After uRPF is enabled on interfaces, a uRPF check is performed for all packets received on physical ports corresponding to these interfaces, which increases the scope of packets checked by uRPF. If a packet received on a tunnel port is also received on the preceding physical ports, the packet is also checked by uRPF. In such a scenario, be cautious in enabling uRPF.

- After uRPF is enabled, the route forwarding capacity of a device will be reduced by half.
- After the uRPF strict mode is enabled, if a packet received on an interface matches an equal-cost route during the uRPF check, the packet will be processed according to the URPF loose mode.
- If uRPF is configured in global configuration mode, the default route cannot be used for a uRPF check.
- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.
- uRPF cannot be enabled on a range of interfaces.

Examples

The following example enables uRPF on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip verify urpf drop-rate compute interval

Function

Run the **ip verify urpf drop-rate compute interval** command to configure the interval for calculating the uRPF IPv4/IPv6 packet loss rate.

Run the **no** form of this command to remove this configuration.

The default interval for calculating the uRPF IPv4/IPv6 packet loss rate is **30** seconds.

Syntax

ip verify urpf drop-rate compute interval *interval*

no ip verify urpf drop-rate compute interval

Parameter Description

interval *interval*: Specifies the interval for calculating the uRPF packet loss rate, in seconds. The value range is from 30 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The interval for calculating the uRPF packet loss rate is configured in global configuration mode, which applies to the calculation of the uRPF packet loss rate globally and on each interface with uRPF enabled and takes effect to IPv4 and IPv6 uRPF.

Examples

The following example sets the interval for calculating the uRPF IPv4/IPv6 packet loss rate to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify urpf drop-rate compute interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip verify urpf drop-rate notify**
- **ip verify urpf drop-rate notify hold-down**

1.5 ip verify urpf drop-rate notify

Function

Run the **ip verify urpf drop-rate notify** command to enable uPRF packet loss information monitoring.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

uRPF packet loss information monitoring is disabled by default.

Syntax

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

default ip verify urpf drop-rate notify

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After uRPF packet loss information monitoring is enabled, a device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the uRPF check so that the users can monitor the network status conveniently.

Examples

The following example enables uRPF packet loss information monitoring on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip verify urpf drop-rate compute interval**
- **ip verify urpf drop-rate notify hold-down**

1.6 ip verify urpf drop-rate notify hold-down

Function

Run the **ip verify urpf drop-rate notify hold-down** command to configure the alarm interval of the uRPF IPv4/IPv6 packet loss rate.

Run the **no** form of this command to remove this configuration.

The default alarm interval for the uRPF IPv4/IPv6 packet loss rate is **300** seconds.

Syntax

ip verify urpf drop-rate notify hold-down *hold-down-time*

no ip verify urpf drop-rate notify hold-down

Parameter Description

hold-down *hold-down-time*: Specifies the alarm interval of the uRPF packet loss rate, in seconds. The value range is from 30 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The alarm interval of the uRPF packet loss rate is configured in global configuration mode, and applies to alarm reporting of the uRPF packet loss rate globally and on each interface with uRPF enabled and takes effect to IPv4 and IPv6 uRPF.

Examples

The following example sets the alarm interval of the uRPF IPv4/IPv6 packet loss rate to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify urpf drop-rate notify hold-down 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip verify urpf drop-rate compute interval**
- **ip verify urpf drop-rate notify**

1.7 ip verify urpf notification threshold

Function

Run the **ip verify urpf notification threshold** command to configure the threshold of the uRPF packet loss rate.

Run the **no** form of this command to remove this configuration.

The default threshold of the uRPF packet loss rate is **1000** packets per second.

Syntax

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

Parameter Description

threshold *rate-value*: Specifies the threshold of the uRPF packet loss rate, in packets per second. The value range is from 0 to 4294967295. If the threshold is **0**, a notification is sent for every packet that is discarded because it fails in the uRPF check.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the threshold of the uRPF packet loss rate to 10 packets per second on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf notification threshold 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show ip urpf

Function

Run the **show ip urpf** command to display the IPv4 uRPF configurations and statistics.

Syntax

show ip urpf [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose configurations and statistics are displayed. If this parameter is not specified, configurations and statistics of all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the uRPF configurations and statistics on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ip urpf interface gigabitethernet0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

The following example displays IPv4 uRPF configurations and statistics on all interfaces.

```
Hostname> enable
Hostname# show ip urpf
IP verify URPF drop-rate compute interval is 30s
IP verify URPF drop-rate notify hold-down is 300s
Interface GigabitEthernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

Table 1-1 Output Fields of the show ip urpf Command

Field	Description
IP verify URPF drop-rate compute interval is x	Interval for calculating the packet loss rate
IP verify URPF drop-rate notify hold-down is x	Alarm interval of the packet loss rate
Interface *interface-type interface-number*	Type and number of the interface whose uRPF configurations and statistics are displayed
IP verify source reachable-via *mode*	● When *mode* is set to **RX**, the uRPF strict mode is used. ● When *mode* is set to **ANY**, the uRPF loose mode is used.
IP verify URPF drop-rate notify *status*	Packet loss information monitoring status: ● When *status* is set to **enabled**, packet loss information monitoring is enabled. ● When *status* is set to **disabled**, packet loss information monitoring is disabled.
IP verify URPF notification threshold is *number*pps	Threshold of the uRPF packet loss rate
Number of drop packets in this interface is *number*	Number of lost packets
Number of drop-rate notification counts in this interface is *count*	Number of notifications for uRPF packet loss information monitoring

Notifications

N/A

Platform Description

N/A

1 DoS Protection Commands

Command	Function
ip deny invalid-l4port	Enable the function of denying invalid L4 ports.
ip deny invalid-tcp	Enable the function of denying invalid TCP packets.
ip deny land	Enable the function of denying land attacks.
show ip deny	Display the status of an anti-denial-of-service (DoS) attack function.

1.1 ip deny invalid-l4port

Function

Run the **ip deny invalid-l4port** command to enable the function of denying invalid L4 ports.

Run the **no** form of this command to disable this feature.

The function of denying invalid L4 ports is disabled by default.

Syntax

ip deny invalid-l4port

no ip deny invalid-l4port

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of denying invalid L4 ports.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip deny invalid-l4port
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip deny invalid-tcp

Function

Run the **ip deny invalid-tcp** command to enable the function of denying invalid TCP packets.

Run the **no** form of this command to disable this feature.

The function of denying invalid TCP packets is disabled by default.

Syntax

ip deny invalid-tcp

no ip deny invalid-tcp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of denying invalid TCP packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip deny invalid-tcp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip deny land

Function

Run the **ip deny land** command to enable the function of denying land attacks.

Run the **no** form of this command to disable this feature.

The function of denying land attacks is disabled by default.

Syntax

ip deny land

no ip deny land

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of denying land attacks.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip deny land
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show ip deny

Function

Run the **show ip deny** command to display the status of an anti-denial-of-service (DoS) attack function.

Syntax

show ip deny [**invalid-l4port** | **invalid-tcp** | **land**]

Parameter Description

invalid-l4port: Displays the status of the function of denying invalid L4 ports.

invalid-tcp: Displays the status of the function of denying invalid TCP packets.

land: Displays the status of the function of denying land attacks.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statuses of all anti-DoS attack functions.

```
Hostname> enable
Hostname# show ip deny
DoS Protection Mode                    State
-------------------------------------    -----
Protect against Land attack             On
Protect against invalid L4port attack    Off
Protect against invalid TCP attack       Off
Protect against null-scan attack         Off
```

Table 1-1 Output Fields of the show ip deny Command

Field	Description
Protect against Land attack	Status of the function of denying land attacks: ● **On**: The function is enabled. ● **Off**: The function is disabled.
Protect against invalid L4port attack	Status of the function of denying invalid L4 ports: ● **On**: The function is enabled. ● **Off**: The function is disabled.
Protect against invalid TCP attack	Status of the function of denying invalid TCP packets: ● **On**: The function is enabled. ● **Off**: The function is disabled.
Protect against null-scan attack	Status of the function of denying null scan attacks: ● **On**: The function is enabled. ● **Off**: The function is disabled.

Notifications

N/A

Platform Description

N/A

Related Commands

- **ip deny invalid-l4port**
- **ip deny invalid-tcp**
- **ip deny land**

1 Security Log Auditing Commands

Command	Function
security-log audit-enable	Enable security log auditing.
security-log auto-vacuum-time	Configure the handling time of aged security logs.
security-log data-store-days	Configure the local storage time of security logs.
security-log data-store-items	Configure the local storage capacity for security logs.
security-log delete all	Clear logs for all key operations.
show security-log	Display all security logs.
show security-log config	Display security log configurations.
show security-log detail	Display detailed security log information.
show security-log detail export	Display detailed security log information.
show security-log detail stat	Display detailed security log statistics.
show security-log info	Display statistics during log processing.
show security-log statistics	Display security log statistics.

1.1 security-log audit-enable

Function

Run the **security-log audit-enable** command to enable security log auditing.

Run the **no** form of this command to disable this feature.

Security log auditing is enabled by default.

Syntax

security-log audit-enable

no security-log audit-enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

After the security log auditing function is enabled, the device records logs for key operations, including account management, login events, system events, configuration file changes, and auditing events.

Examples

The following example enables security log auditing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log audit-enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 security-log auto-vacuum-time

Function

Run the **security-log auto-vacuum-time** command to configure the handling time of aged security logs.

The default handling time of aged security logs is **03:00:00** every day.

Syntax

security-log auto-vacuum-time *hh*:*mm*:*ss*

Parameter Description

hh:*mm*:*ss*: Handling time of aged security logs. Here, *hh* indicates the hour, *mm* indicates the minute, and *ss* indicates the second.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to configure the time for checking local logs. By default, the system checks whether any local logs have exceeded the storage time at 03:00:00 every day and deletes expired logs.

Examples

The following example sets the handling time for aged security logs to 05:05:00 every day.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log auto-vacuum-time 05:05:00
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 security-log data-store-days

Function

Run the **security-log data-store-days** command to configure the local storage time of security logs.

The default local storage time of security logs is **65535** days.

Syntax

security-log data-store-days *data-store-time*

Parameter Description

data-store-time: Local storage time of security logs, in days. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- This command is used to configure the local storage time of security logs.
- The security logs for key operations are stored in the local database for **65535** days by default, and expired logs will be deleted.

Examples

The following example sets the local storage time of security logs to 300 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log data-store-days 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 security-log data-store-items

Function

Run the **security-log data-store-items** command to configure the local storage capacity for security logs.

The maximum and minimum local storage capacity for security logs are **10000** and **500** (standard security requirements), respectively by default.

Syntax

security-log data-store-items *log-number*

Parameter Description

log-number: Local storage capacity for security logs. The value range is from 500 to 10000.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If the local storage space is insufficient, you can run this command to decrease the storage capacity for security logs.

Examples

The following example sets the local storage capacity for security logs to 5000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log data-store-items 5000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 security-log delete all

Function

Run the **security-log delete all** command to clear logs for all key operations.

Syntax

security-log delete all

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example clears logs for all key operations.

```
Hostname> enable
Hostname# security-log delete all
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show security-log

Function

Run the **show security-log** command to display all security logs.

Syntax

show security-log

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays all security logs.

```
Hostname> enable
Hostname# show security-log
time, username, peerinfo, hostname, log-type: content
```

```
2019-01-01 10:00:02, -, console, Hostname, SEC_LOG: SECURITY_LOG enabled security log
audit configuration successfully
2019-01-01 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG
disabled security log audit configuration unsuccessfully
2019-01-01 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG
deleted all security log successfully
……
```

Table 1-1 Output Fields of the show security-log Command

Field	Description
time	Log generation time
username	Username
peerinfo	Terminal information, including the terminal name, IP address, or both
hostname	Host name
log-type	Log type, including: ● SEC_LOG (security log events) ● ACC_MNT (account management) ● LOGIN (login events) ● SYS (system events) ● CONFIG (configuration file changes) ● OTHER (others)
content	Log content

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show security-log config

Function

Run the **show security-log config** command to display security log configurations.

Syntax

show security-log config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display security log configurations, including whether log auditing is enabled, log capacity limit, log storage time, and handling time for aged security logs.

Examples

The following example displays security log configurations.

```
Hostname> enable
Hostname# show security-log config
Security-log audit: enable
Limit number: 10000
Store days: 180
Auto vacuum time: 03:00:00
Security-log send to syslog: enable
```

Table 1-2 Output Fields of the show security-log config Command

Field	Description
Security-log audit	Status of the security log auditing function: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Limit number	Security log capacity limit
Store days	Security log storage days
Auto vacuum time	Handling time of aged security logs
Security-log send to syslog	Status of the function of sending security logs to the syslog server

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show security-log detail

Function

Run the **show security-log detail** command to display detailed security log information.

Syntax

show security-log detail { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }

Parameter Description

all: Displays all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are displayed. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are displayed.

log-type: Specifies the log type based on which security logs are displayed. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are displayed. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are displayed.

order-by log-type: Orders logs by log type.

order-by time: Orders logs by log time.

asc: Orders logs in ascending mode.

desc: Orders logs in descending mode.

start-item *start-item*: Specifies the start position in the search result. The value range is from 1 to 10000.

end-item *end-item*: Specifies the end position in the search result. The value range is from 1 to 10000.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

Examples

The following example displays all security logs.

```
Hostname> enable
Hostname# show security-log detail all
time, username, peerinfo, hostname, log-type: content
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG deleted all security log successfully
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG disabled security log audit configuration unsuccessfully
2019-10-22 10:00:03, -, console, Hostname, SEC_LOG: SECURITY_LOG enabled security log audit configuration successfully
……
```

Table 1-3 Output Fields of the show security-log detail all Command

Field	Description
time	Log generation time
username	Username
peerinfo	Terminal information, including the terminal name, IP address, or both
hostname	Host name
log-type	Log type, including: ● SEC_LOG (security log events) ● ACC_MNT (account management) ● LOGIN (login events) ● SYS (system events) ● CONFIG (configuration file changes) ● OTHER (others)
content	Log content

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show security-log detail export

Function

Run the **show security-log detail export** command to display detailed security log information.

Syntax

show security-log detail export { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }

Parameter Description

all: Exports all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are exported. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are exported.

log-type: Specifies the log type based on which security logs are exported. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are exported. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are exported.

order-by log-type: Orders logs by log type.

order-by time: Orders logs by log time.

asc: Orders logs in ascending mode.

desc: Orders logs in descending mode.

start-item *start-item*: Specifies the start position in the export result. The value range is from 1 to 10000.

end-item *end-item*: Specifies the end position in the export result. The value range is from 1 to 10000.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to export detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

You can run the **copy** command to download the exported file. The following shows an example.

```
Hostname# copy tmp:mng/security_log/export_file/log_20191022_110410_535250.csv
tftp://192.168.1.1/security_log.csv
```

Examples

The following example exports security logs of user A during the time range from 00:00:00 October 10, 2019 to 24:00:00 October 22, 2019.

```
Hostname> enable
Hostname# show security-log detail export from 2019 10 10 00:00:00 to 2019 10 22 23:59:59
user userA
Export file: tmp:mng/security_log/export_file/log_20191022_110410_535250.csv
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show security-log detail stat

Function

Run the **show security-log detail stat** command to display detailed security log statistics.

Syntax

show security-log detail stat { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*]

Parameter Description

all: Displays all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are displayed. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are displayed.

log-type: Specifies the log type based on which security logs are displayed. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are displayed. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display detailed security log statistics, which can be filtered by time, log type, username, host name, and terminal information.

Examples

The following example displays security log statistics of user A during the time range from 00:00:00 October 10, 2019 to 24:00:00 October 22, 2019.

```
Hostname# show security-log detail stat from 2019 10 10 00:00:00 to 2019 10 22 23:59:59
user userA
Count:555
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show security-log info

Function

Run the **show security-log info** command to display statistics during log processing.

Syntax

show security-log info

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays security log statistics.

```
Hostname> enable
Hostname# show security-log info
Receive log count: 2000, err 1
Send syslog count: 1800
Current cached record count: 1999
Current store-in-flash record count: 5000
Historital sync flash count: 100, err 1
Reason for last sync failure: Failed to sync security logs to file database.
Next time to sync flash: 11:11:11
```

Table 1-4 Output Fields of the show security-log info Command

Field	Description
Receive log count	Number of successfully received logs (xxx) and number of logs failed to be received (xxx)
Current cached record count	Number of cached logs
Current store-in-flashrecord count	Number of logs stored in the flash memory
Historital sync flash count	Number of historical synchronization times to the flash memory (xxx) and number of failed synchronizations (xxx)
Reason for last sync failure	Reason for the last synchronization failure (which is displayed if a synchronization failure occurred and not displayed if no synchronization failure occurs)
Next time to sync flash	Next synchronization time to the flash memory, in HH:MM:SS format

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show security-log statistics

Function

Run the **show security-log statistics** command to display security log statistics.

Syntax

show security-log statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display security log statistics, including the number of recorded logs and last deleted log. For details, see Table 1-5.

Examples

The following example displays security log statistics.

```
Hostname> enable
Hostname# show security-log statistics
Current storage record count: 9000
Historical record count: have written 11111, overwritten 1111
Aging record count: 1000
Last delete record: 2019-10-24 10:00:00 userA vty0(192.168.1.1) Hostname SEC_LOG:
SECURITY_LOG deleted all security log successfully
```

Table 1-5 Output Fields of the show security-log statistics Command

Field	Description
Current cache record count	Number of cached logs
Current storage record count	Number of locally stored logs
Historical storage record count	Number of historically stored logs in the local database, including the total number of stored logs (xxx) and the number of overwritten logs (xxx)
Aging record count	Number of aged logs in the local database
Last delete record	Last deleted log

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Reliability Commands

1 REUP Commands

Command	Function
switchport backup interface	Configure a dual-link backup port of Rapid Ethernet Uplink Protection (REUP).
switchport backup interface preemption mode	Configure the link preemption mode of REUP.
switchport backup interface preemption delay	Configure the link preemption delay time of REUP.
mac-address-table update group	Configure a MAC address update group.
mac-address-table move update transit	Enable the function of sending MAC address update private multicast messages.
mac-address-table move update transit vlan	Configure the ID of a VLAN, in which a port sends MAC address update private multicast messages.
mac-address-table move update max-update-rate	Configure the maximum rate for sending MAC address update broadcast packets.
mac-address-table move update receive	Enable the function of receiving MAC address update private multicast messages.
mac-address-table move update receive vlan	Configure a VLAN ID range, in which MAC address update private multicast messages are received.
switchport backup interface prefer instance	Configure VLAN load balancing for a port with REUP dual-link backup enabled.
link state track	Enable a link state tracking group.
link state group	Add a port to a specified link state tracking group.
show interfaces switchport backup	Display the status information of a port with REUP dual-link backup enabled.
show mac-address-table update group	Display the information about a MAC address update group.
show mac-address-table move update	Display the statistics on the MAC address update private multicast messages sent by a port with REUP dual-link backup enabled.
show link state group	Display information about a link state tracking group.

1.1 switchport backup interface

Function

Run the **switchport backup interface** command to configure a dual-link backup port of Rapid Ethernet Uplink Protection (REUP).

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No REUP dual-link backup port is configured by default.

Syntax

switchport backup interface *interface-type interface-number*

no switchport backup interface *interface-type interface-number*

default switchport backup interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Port type and number of the backup link.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When this command is configured, the port where the interface configuration mode is configured is the active port, and the port specified by the *interface-type interface-number* parameter is the backup port. When the active link corresponding to the active port is faulty, the backup port link is enabled to implement rapid recovery.

Examples

The following example configures the REUP dual-link backup function, and configures GigabitEthernet 0/1 as the active port and GigabitEthernet 0/2 as the backup port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2
```

Notifications

If a port is configured as the active port and backup port at the same time, the following notification will be displayed:

```
interface GigabitEthernet 0/1 can not backup itself.
```

If a configured active or backup port has been used to constitute another REUP pair, the following notification will be displayed:

```
interface GigabitEthernet 0/1 have already configured to another reup pair.
```

If the number of configured REUP port pairs reaches the maximum number, the following notification will be displayed:

```
Can not configure more than 16 pair.
```

Common Errors

- The configured active or backup port has been used to constitute another REUP pair.
- When the configured port is not an L2 physical port or L2 aggregate port (AP), this command is not supported.

Platform Description

N/A

Related Commands

N/A

1.2 switchport backup interface preemption mode

Function

Run the **switchport backup interface preemption mode** command to configure the link preemption mode of REUP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default link preemption mode of REUP is off mode.

Syntax

switchport backup interface *interface-type interface-number* **preemption mode** { **bandwidth** | **forced** | **off** }

no switchport backup interface *interface-type interface-number* **preemption mode**

default switchport backup interface *interface-type interface-number* **preemption mode**

Parameter Description

interface-type interface-number: Port type and number of the backup link.

bandwidth: Indicates the bandwidth mode, in which a port with a greater bandwidth is preferred for data transmission.

forced: Indicates the forced mode, in which the active port is preferred for data transmission.

off: Indicates the off mode, in which preemption is not performed.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When this command is configured, if no REUP backup port is configured for an active port, a backup port is automatically configured and added. When the **no** form of this command is run, the backup port is not deleted.

Examples

The following example configures the REUP dual-link backup function, specifies GigabitEthernet 0/1 as the active port and GigabitEthernet 0/2 as the backup port, and sets the link preemption mode of REUP to bandwidth mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 preemption mode bandwidth
```

Notifications

If a port is configured as the active port and backup port at the same time, the following notification will be displayed:

```
interface GigabitEthernet 0/1 can not backup itself.
```

If a configured active or backup port has been used to constitute another REUP pair, the following notification will be displayed:

```
interface GigabitEthernet 0/1 have already configured to another reup pair.
```

Common Errors

- The configured active or backup port has been used to constitute another REUP pair.
- When the configured port is not an L2 physical port or L2 AP, this command is not supported.

Platform Description

N/A

Related Commands

- **switchport backup interface**

1.3 switchport backup interface preemption delay

Function

Run the **switchport backup interface preemption delay** command to configure the link preemption delay time of REUP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default preemption delay time of REUP is **35** seconds.

Syntax

switchport backup interface *interface-type interface-number* **preemption delay** *interval*

no switchport backup interface *interface-type interface-number* **preemption delay**

default switchport backup interface *interface-type interface-number* **preemption delay**

Parameter Description

interface-type interface-number: Port type and number of the backup link.

interval: Delay time for link preemption, in seconds. The value range is from 1 to 300.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Preemption delay indicates the delay time for link switching after a faulty link recovers.

It is effective only in bandwidth and forced preemption modes.

When this command is configured, if no REUP backup port is configured for an active port, a backup port is automatically configured and added. When the **no** form of this command is run, the backup port is not deleted.

Examples

The following example configures the REUP dual link backup function, specifies GigabitEthernet 0/1 as the active port and GigabitEthernet 0/2 as the backup port, and sets the link preemption mode of REUP to forced mode and the link preemption delay time to 40s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 preemption mode forced
Hostname(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 preemption delay 40
```

Notifications

If a port is configured as the active port and backup port at the same time, the following notification will be displayed:

```
interface GigabitEthernet 0/1 can not backup itself.
```

If a configured active or backup port has been used to constitute another REUP pair, the following notification will be displayed:

```
interface GigabitEthernet 0/1 have already configured to another reup pair.
```

Common Errors

- The configured active or backup port has been used to constitute another REUP pair.
- When the configured port is not an L2 physical port or L2 AP, this command is not supported.

Platform Description

N/A

Related Commands

- **switchport backup interface**
- **switchport backup interface preemption mode**

1.4 mac-address-table update group

Function

Run the **mac-address-table update group** command to configure a MAC address update group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No MAC address update group is configured by default.

Syntax

mac-address-table update group [*group-id*]

no mac-address-table update group [*group-id*]

default mac-address-table update group [*group-id*]

Parameter Description

group-id: ID of a MAC address update group. The value range is from 1 to 8, and the default value is **1**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To restore data transmission quickly after link switching, you can use the MAC address update advertising function. MAC address updates can cause massive broadcast packet flooding, which affects normal data transmission of the device. To prevent this consequence, you only need to add all ports in a switching path to the same MAC address update group so that the MAC address changes are synchronized in the group to achieve instant recovery.

Running the **no** and **default** forms of the command without specifying any parameters means that the configuration takes effect in all the update groups.

One port can belong to multiple MAC address update groups, and different types of ports can belong to the same MAC address update group.

Examples

The following example adds port GigabitEthernet 0/1 and GigabitEthernet 0/2 to MAC address update group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface range gigabitethernet 0/1-2
Hostname(config-if-range)# mac-address-table update group 1
```

Notifications

If the number of member ports in a MAC address update group reaches the maximum value, the following notification will be displayed:

```
Can not configure more than 8 member for a flush group.
```

Common Errors

- The configured MAC address update group ID is not within the allowed value range.
- When the configured port is not an L2 physical port or L2 AP, this command is not supported.

Platform Description

N/A

Related Commands

N/A

1.5 mac-address-table move update transit

Function

Run the **mac-address-table move update transit** command to enable the function of sending MAC address update private multicast messages.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No MAC address update private multicast message is sent by default.

Syntax

mac-address-table move update transit

no mac-address-table move update transit

default mac-address-table move update transit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To reduce data loss in downstream data streams during link switching, you need to enable the function of sending MAC address update private multicast messages on the device where link switching occurs.

Examples

The following example enables the function of sending MAC address update private multicast messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table move update transit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 mac-address-table move update transit vlan

Function

Run the **mac-address-table move update transit vlan** command to configure the ID of a VLAN, in which a port sends MAC address update private multicast messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the VLAN, in which a port sends MAC address update private multicast messages, is the default VLAN of the port.

Syntax

mac-address-table move update transit vlan *vlan-id*

no mac-address-table move update transit vlan

default mac-address-table move update transit vlan

Parameter Description

vlan-id: ID of a VLAN, in which a port sends MAC address update private multicast messages.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the REUP dual-link backup and the function of sending MAC address update private multicast messages have been configured on a device, when link switching is performed, the device sends the MAC address update private multicast message that carries a specified VLAN ID to the uplink device.

Examples

The following example sets the ID of a VLAN, in which port GigabitEthernet 0/1 sends MAC address update private multicast messages to 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac-address-table move update transit vlan 10
```

Notifications

If REUP is not configured for the local port, the following notification will be displayed:

```
Please enable REUP first.
```

Common Errors

- REUP is not configured for the local port.

Platform Description

N/A

Related Commands

- **switchport backup interface**
- **mac-address-table move update transit**

1.7 mac-address-table move update max-update-rate

Function

Run the **mac-address-table move update max-update-rate** command to configure the maximum rate for sending MAC address update broadcast packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default maximum rate for sending MAC address update broadcast packets is **150** packets/second.

Syntax

mac-address-table move update max-update-rate *packet-per-second*

no mac-address-table move update max-update-rate

default mac-address-table move update max-update-rate

Parameter Description

packet-per-second: Maximum rate for sending MAC address update broadcast packets, in packets per second. The value range is from 0 to 32000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If a device has been configured with REUP dual-link backup, when link switching is performed, a MAC address update broadcast packet is sent to the uplink device at the configured maximum rate to quickly recover downlink data transmission of the uplink device.

When the uplink device is another vendor's device (which does not support receiving MAC address update private multicast messages), the downlink device updates the MAC address by using the default policy (sending broadcast packets regularly), and this command is used to configure the maximum sending rate.

Examples

The following example sets the maximum rate for sending MAC address update packets to 20 packets/second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table move update max-update-rate 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 mac-address-table move update receive

Function

Run the **mac-address-table move update receive** command to enable the function of receiving MAC address update private multicast messages.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No MAC address update private multicast message is received by default.

Syntax

mac-address-table move update receive

no mac-address-table move update receive

default mac-address-table move update receive

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When link switching occurs on a device with REUP dual-link backup enabled, forwarding of the downstream data streams is interrupted because the MAC address table of the uplink device is not updated in time. To reduce the interruption time of L2 data streams, the MAC address table of the uplink device can be updated quickly to resume forwarding. Therefore, you need to enable the function of sending MAC address update private multicast messages on the device with dual-link backup enabled and enable the function of receiving MAC address update private multicast messages on the uplink device.

Examples

The following example enables the function of receiving MAC address update private multicast messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac-address-table move update receive
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 mac-address-table move update receive vlan

Function

Run the **mac-address-table move update receive vlan** command to configure a VLAN ID range, in which MAC address update private multicast messages are received.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The MAC address update private multicast messages in all the VLAN ID ranges are received by default.

Syntax

mac-address-table move update receive vlan *vlan-range*

no mac-address-table move update receive [**vlan** *vlan-range*]

default mac-address-table move update receive [**vlan** *vlan-range*]

Parameter Description

vlan-range: String of the VLAN ID range, in which MAC address update private multicast messages are received. "-" indicates a continuous range, and "," indicates discrete values. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to disable the function of receiving the MAC address update private multicast messages in some VLANs. For a VLAN with the function of receiving MAC address update private multicast messages disabled, MAC address update broadcast packets can be used to recover downlink transmission of the uplink device, but the convergence performance will be decreased in the case of link faults.

The VLAN ID range configured using this command is the incremental configuration. If you need to configure the function of receiving only the MAC address update private multicast messages of a certain VLAN range segment, delete all the VLAN range segments first, and then configure a new VLAN range segment.

Examples

The following example configures the function of receiving the MAC address update private multicast messages of VLAN 10 only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no mac-address-table move update receive vlan 1-4094
Hostname(config)# mac-address-table move update receive vlan 10
```

Notifications

If the format of the entered VLAN is incorrect, the following notification will be displayed:

```
% Invalid input detected at '^' marker.
```

Common Errors

- The format of the entered VLAN is incorrect.

Platform Description

N/A

Related Commands

- **mac-address-table move update receive**

1.10 switchport backup interface prefer instance

Function

Run the **switchport backup interface prefer instance** command to configure VLAN load balancing for a port with REUP dual-link backup enabled.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no VLAN load balancing is configured for a port with REUP dual-link backup enabled.

Syntax

switchport backup interface *interface-type interface-number* **prefer instance** *instance-range*

no switchport backup interface *interface-type interface-number* **prefer**

default switchport backup interface *interface-type interface-number* **prefer**

Parameter Description

interface-type interface-number: Port type and number of the backup link.

instance-range: Range of instances with VLAN load balancing enabled.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can modify the mappings between instances and VLANs by using the instance mapping function of Multiple Spanning Tree Protocol (MSTP).

When this command is configured, if no REUP backup port is configured for an active port, a backup port is automatically configured and added. When the **no** form of this command is run, the backup port is not deleted.

Examples

The following example configures the REUP dual-link backup function, specifies GigabitEthernet 0/1 as the active port and GigabitEthernet 0/2 as the backup port, and configures VLAN load balancing on instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 prefer instance 1
```

Notifications

If the port is not in the trunk/hybrid/uplink mode, the following notification will be displayed:

```
Reup vlan loadbalance only support interface on trunk, hybrid or uplink mode.
```

If a port is configured as the active port and backup port at the same time, the following notification will be displayed:

```
interface GigabitEthernet 0/1 can not backup itself.
```

If a configured active or backup port has been used to constitute another REUP pair, the following notification will be displayed:

```
interface GigabitEthernet 0/1 have already configured to another reup pair.
```

If the number of configured instances associated with MSTP reaches the maximum value, the following notification will be displayed:

```
Instance range error, right range is 0-64
```

Common Errors

- The command is configured in the trunk/hybrid/uplink mode on a non-L2 port.
- The number of instances associated with MSTP reaches the maximum value.

Platform Description

N/A

Related Commands

- **switchport backup interface**
- **instance** (Ethernet switching/MSTP)

1.11 link state track

Function

Run the **link state track** command to enable a link state tracking group.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

All the link state tracking groups are disabled by default.

Syntax

link state track [*track-number* | **up-delay** *interval*]

no link state track [*track-number*]

default link state track [*track-number*]

Parameter Description

track-number: ID of a link state tracking group. The value range is from 1 to 2, and the default value is **1**.

up-delay *interval*: Configures the delay time for downlink recovery, in seconds. The value range is 0 to 300, and the default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You must create a link state tracking group first and then add a port to the tracking group.

If no parameter is specified, the default link state tracking group 1 is enabled.

Examples

The following example enables link state tracking group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# link state track 1
```

The following example enables link state tracking group 1, and configures the downlink to recover with a delay of 30s after the uplink recovers.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# link state track 1 up-delay 30
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 link state group

Function

Run the **link state group** command to add a port to a specified link state tracking group.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No port is added to a link state tracking group by default.

Syntax

link state group [*track-number*] { **upstream** | **downstream** }

no link state group

default link state group

Parameter Description

track-number: ID of a link state tracking group. The value range is from 1 to 2, and the default value is **1**. If this parameter is not specified, the link state tracking group ID is 1.

upstream: Configures an upstream port in the link state tracking group.

downstream: Configures a downstream port in the link state tracking group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You must enable a link state tracking group and add a port to the tracking group before this command takes effect.

Examples

The following example enables link state tracking group 1, adds port GigabitEthernet 0/1 as an upstream port of link state tracking group 1 and port GigabitEthernet 0/2 as a downstream port of link state tracking group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# link state track 1
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# link state group 1 upstream
Hostname(config-if-GigabitEthernet 0/1)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# link state group 1 downstream
```

Notifications

If a port has been configured as a port of a link state tracking group, the following notification will be displayed:

```
Have configured a link state group for this interface GigabitEthernet 0/1.
```

If the number of upstream ports in a link state tracking group reaches the maximum value, the following notification will be displayed:

```
Can not configure more than 8 uplink member for lst group.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **link state track**

1.13 show interfaces switchport backup

Function

Run the **show interfaces switchport backup** command to display the status information of a port with REUP dual-link backup enabled.

Syntax

show interfaces [*interface-type interface-number*] **switchport backup** [**detail**]

Parameter Description

interface-type interface-number: Port type and number. After this parameter is specified, information about the REUP dual-link backup port of a specified port type and number is displayed.

detail: Displays the details of a port with REUP dual-link backup enabled. If this parameter is not specified, the brief information of a port with REUP dual-link backup enabled is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the brief information of all the ports with REUP dual-link backup enabled.

```
Hostname> enable
Hostname# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface        Backup Interface       State
------------------------------------------------------------------------
Gi0/1                Gi0/2                Active Down/Backup Down
Gi0/3                Gi0/4                Active Down/Backup Down
Gi0/5                Ag1                 Active Down/Backup Down
```

The following example displays the details of all the ports with REUP dual-link backup enabled.

```
Hostname> enable
Hostname# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active Interface        Backup Interface       State
------------------------------------------------------------------------
Gi0/1                Gi0/2                Active Down/Backup Down
Gi0/3                Gi0/4                Active Down/Backup Down
Gi0/5                Ag1                 Active Down/Backup Down

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(1000 Mbits)
```

```
Interface Pair : Gi0/3, Gi0/4
Preemption Mode : forced
Preemption Delay : 120 seconds
Bandwidth : Gi0/3(1000 Mbits), Gi0/4(1000 Mbits)

Interface Pair : Gi0/5, Ag1
Preemption Mode : bandwidth
Preemption Delay : 180 seconds
Bandwidth : Gi0/5(1000 Mbits), Ag1(10000 Mbits)
```

The following example displays the details of port GigabitEthernet 0/1 with REUP dual-link backup enabled.

```
Hostname> enable
Hostname# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
Gi0/1                Gi0/2                Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 50 seconds
Bandwidth : Gi0/1 (1000 Mbits), Gi0/2(1000 Mbits)
```

Table 1-1 Output Fields of the show interfaces switchport backup Command

Field	Description
Active Interface	Active port
Backup Interface	Backup port
State	Member port state (**Active** indicates an active port and **Backup** indicates a backup port): ● **Up**: Indicates the forwarding state. ● **Standby**: Indicates the blocked state. ● **Down**: Indicates that the port link is down. ● **Error**: Indicates unknown state.
Interface Pair	Member port list

Field	Description
Preemption Mode	Link preemption mode: ● **Forced**: Indicates forced mode, in which the active port is preferred for data transmission. ● **Bandwidth**: Indicates bandwidth mode, in which the port with a greater bandwidth is preferred for data transmission. ● **Off**: Indicates that the preemption mode is off, namely, no preemption is performed.
Preemption Delay	Link preemption delay, indicating the delay time for link switching after the faulty link recovers
Bandwidth	Bandwidth of the member port

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show mac-address-table update group

Function

Run the **show mac-address-table update group** command to display the information about a MAC address update group.

Syntax

show mac-address-table update group [**detail**]

Parameter Description

detail: Displays the details of a MAC address update group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the brief information of a MAC address update group.

```
Hostname>
Hostname# show mac-address-table update group

Mac-address-table Update Group:1
Member:Gi0/1, Gi0/2
```

The following example displays the details of a MAC address update group.

```
Hostname>
Hostname# show mac-address-table update group detail

Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count    Last Receive Switch-ID      Receive Time
Gi0/1               0              0000.0000.0000
Gi0/2               0              0000.0000.0000
```

Table 1-2 Output Fields of the show mac-address-table update group Command

Field	Description
Mac-address-table Update Group	ID of a MAC address update group
Received mac-address-table update message count	Number of the MAC address update private multicast messages received by the MAC address update group
Group member	Member port
Receive Count	Number of the MAC address update private multicast messages received by the member port
Last Receive Switch-ID	Device MAC address in the MAC address update private multicast message received by the member port last time
Receive Time	Time when the member port receives a MAC address update private multicast message last time

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show mac-address-table move update

Function

Run the **show mac-address-table move update** command to display the statistics on the MAC address update private multicast messages sent by a port with REUP dual-link backup enabled.

Syntax

show mac-address-table move update

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics on the MAC address update private multicast messages sent by a port with REUP dual-link backup enabled.

```
Hostname> enable
Hostname# show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:enable
Max-update-rate:150
Receive vlan:1-4094

Pair: Gi0/1,Gi0/2
Members            Status    Transit Count    Transit VLAN   Last Transit Time
-------------------------------------------------------------------------------
--------------
Gi0/1              Down      0
Gi0/2              Down      0
Pair: Ag1,Ag2
Members            Status    Transit Count    Transit VLAN   Last Transit Time
-------------------------------------------------------------------------------
--------------
Ag1                Down      0
Ag2                Down      0
Pair: Gi0/3,Ag3
Members            Status    Transit Count    Transit VLAN   Last Transit Time
```

```
--------------------------------------------------------------------------------
--------------
Gi0/3               Down      0
Ag3                 Down      0
```

Table 1-3 Output Fields of the show mac-address-table move update Command

Field	Description
Transit	Whether the function of sending MAC address update private multicast messages globally is enabled: ● **enable**: Indicates that the function is enabled. ● **disable**: Indicates that the function is disabled.
Receive	Whether the function of receiving MAC address update private multicast messages globally is enabled: ● **enable**: Indicates that the function is enabled. ● **disable**: Indicates that the function is disabled.
Max-update-rate	Maximum rate for sending MAC address update broadcast packets, in packets per second
Receive vlan	VLAN ID range for receiving MAC address update private multicast messages
Pair	REUP port pair
Members	Members of the REUP port pair
Status	Status of a member port: ● **Up**: Indicates the forwarding state. ● **Standby**: Indicates the blocked state. ● **Down**: Indicates that the port link is down. ● **Error**: Indicates unknown state.
Transit Count	Number of the MAC address update private multicast messages sent by the member port.
Transit VLAN	VLAN range, in which MAC address update private multicast messages are sent by the member port
Last Transit Time	Time when the member port sends a MAC address update private multicast message last time

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show link state group

Function

Run the **show link state group** command to display information about a link state tracking group.

Syntax

show link state group

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about a link state tracking group.

```
Hostname> enable
Hostname# show link state group

Link State Group:1  Status: Enabled, Down
Up-delay (default 0s): 0(s)
Upstream Interfaces :Gi0/1(Down),Gi0/2(Down)
Downstream Interfaces :Gi0/3(Down)

Link State Group:2  Status: Disabled, Down
Up-delay (default 0s): 0(s)
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up   (Down):Interface Down   (Dis):Interface disabled
```

Table 1-4 Output Fields of the show link state group Command

Field	Description
Link State Group	ID of a link state tracking group

Field	Description
Status	Status of the link state tracking group: ● **Enabled**: Indicates that the link state tracking group is enabled. ● **Disabled**: Indicates that the link state tracking group is disabled. Working status of the link state tracking group: ● **Up**: Indicates that there is an upstream port with the link in the up status in the tracking group. ● **Down**: Indicates that there is no upstream port with the link in the up status in the tracking group.
Upstream Interfaces	Status of the upstream member port: ● **Up**: Indicates that the port link is in the up status. ● **Down**: Indicates that the port link is in the down status.
Downstream Interfaces	Status of the downstream member port: ● **Dis**: Indicates that the port is in error-disabled status. ● **Up**: Indicates that the port link is in the up status. ● **Down**: Indicates that the port link is in the down status. ● **ERROR**: Indicates that the port status is abnormal.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 RLDP Commands

Command	Function
rldp detect-interval	Configure an interval for sending Rapid Link Detection Protocol (RLDP) packets by a port.
rldp detect-max	Configure the maximum detection count of RLDP.
rldp enable	Enable the global RLDP detection function.
rldp error-recover interval	Configure a time interval for RLDP to recover failed ports.
rldp neighbor-negotiation	Enable the neighbor negotiation function of RLDP.
rldp port	Enable RLDP detection on a port.
rldp reset	Recover all the failed RLDP ports and restart detection.
show rldp	Display the RLDP state information.
rldp detect-latency	Configure the loop detection latency interval of RLDP.

1.1 rldp detect-interval

Function

Run the **rldp detect-interval** command to configure an interval for sending Rapid Link Detection Protocol (RLDP) packets by a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default interval for sending RLDP packets by a port is **3** seconds.

Syntax

rldp detect-interval *interval*

no rldp detect-interval

default rldp detect-interval

Parameter Description

interval: Interval for sending RLDP packets by a port, in seconds. The value range is from 1 to 15.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The command takes effect for the probe packets and loop packets only.

If Spanning Tree Protocol (STP) has been enabled, you are advised to configure the command according to the rule that the total time calculated using the formula of [(Detection interval × Maximum detection count)] + 1 is smaller than the topology convergence time of STP.

Examples

The following example sets the interval for sending RLDP packets by a port to 5 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp detect-interval 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 rldp detect-max

Function

Run the **rldp detect-max** command to configure the maximum detection count of RLDP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default maximum detection count of RLDP is **2**.

Syntax

rldp detect-max *max-detect-number*

no rldp detect-max

default rldp detect-max

Parameter Description

max-detect-number: Maximum detection count of RLDP. The value range is from 2 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Maximum detection time = (Detection interval × Maximum detection count) + 1.

If a neighbor port still fails to respond when the maximum detection time expires, the link is diagnosed as a faulty link.

Examples

The following example sets the maximum detection count of RLDP to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp detect-max 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 rldp enable

Function

Run the **rldp enable** command to enable the global RLDP detection function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The global RLDP detection function is disabled by default.

Syntax

rldp enable

no rldp enable

default rldp enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Only when the global RLDP detection function is enabled, can RLDP detection take effect on a port.

Examples

The following example enables the global RLDP detection function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 rldp error-recover interval

Function

Run the **rldp error-recover interval** command to configure a time interval for RLDP to recover failed ports.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No time interval for RLDP to recover failed ports regularly is configured by default.

Syntax

rldp error-recover interval *interval*

no rldp error-recover interval

default rldp error-recover interval

Parameter Description

interval: Time interval, in seconds. The value range is from 30 to 86400.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to recover failed ports regularly by RLDP.

When an RLDP port is in the error state, RLDP detection is started regularly on the port. If the error has been eliminated, the RLDP port is updated to the normal status; if the error still exists, RLDP detection is still effective on the port, and detection is restarted in the next cycle until the error is removed.

Examples

The following example sets a time interval for RLDP to recover failed ports to 600 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp error-recover interval 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 rldp neighbor-negotiation

Function

Run the **rldp neighbor-negotiation** command to enable the neighbor negotiation function of RLDP.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The neighbor negotiation function is disabled by default.

Syntax

rldp neighbor-negotiation

no rldp neighbor-negotiation

default rldp neighbor-negotiation

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the negotiation function of RLDP is enabled, if a RLDP packet sent by a neighbor is successfully received, it is determined that the negotiation succeeds.

When the negotiation succeeds, the RLDP detection function is started on the port; otherwise, it is not started.

Examples

The following example configures the neighbor negotiation function during RLDP detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp neighbor-negotiation
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 rldp port

Function

Run the **rldp port** command to enable RLDP detection on a port.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

RLDP detection is not configured on a port by default.

Syntax

rldp port { **bidirection-detect** | **loop-detect** | **unidirection-detect** } { **block** | **shutdown-port** | **shutdown-svi** | **warning** }

no rldp port { **bidirection-detect** | **loop-detect** | **unidirection-detect** }

default rldp port { **bidirection-detect** | **loop-detect** | **unidirection-detect** }

Parameter Description

bidirection-detect: Configures bidirectional link detection.

loop-detect: Configures loop detection.

unidirection-detect: Configures unidirectional link detection.

block: Disables the MAC address learning and forwarding functions on the port.

shutdown-port: Shuts down the port.

shutdown-svi: Shuts down the switch virtual interface (SVI) where the port is.

warning: Sends an alarm.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command can be configured on L2 and L3 physical ports.

Aggregate ports (APs) do not support this command, but the command can be configured on the member ports of an AP.

Examples

The following example enables RLDP detection on port GigabitEthernet 0/1, configures the loop detection type, and sets the failure handling method to block.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# rldp port loop-detect block
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 rldp reset

Function

Run the **rldp reset** command to recover all the failed RLDP ports and restart detection.

Syntax

rldp reset

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

This command is used to restore the status of all failed ports, which can also be restored using the **errdisable recovery** command. For the introduction and specific configuration of the **errdisable recovery** command, refer to "Configuring Ethernet Interface" in *Interface Configuration Guide*.

Examples

The following example recovers all the failed RLDP ports and restarts detection.

```
Hostname> enable
Hostname# rldp reset
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show rldp

Function

Run the **show rldp** command to display the RLDP state information.

Syntax

show rldp [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Configures the RLDP port type and number. If this parameter is not specified, the RLDP state information of all the ports is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the RLDP state information of all the ports.

```
Hostname> enable
Hostname# show rldp
rldp state       : disable
rldp hello interval: 3
rldp max hello    : 2
rldp local bridge  : 00d0.f822.37da
GigabitEthernet 0/1
port state     : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal
```

```
loop detect information:
    action: shutdown-port
    state : normal
```

Table 1-1 Output Fields of the show rldp Command

Field	Description
rldp state	State of the global RLDP function: ● **enable**: Indicates that the function is enabled. ● **disable**: Indicates that the function is disabled.
rldp hello interval	Interval for sending RLDP packets by a port, in seconds.
rldp max hello	Maximum detection count of RLDP.
rldp local bridge	MAC address of the local system. It is used to differentiate the local device from the neighbor device.
port state	Port state: ● **error**: Indicates that the link is abnormal. ● **normal**: Indicates that the link is normal.
neighbor bridge	MAC address of the neighbor system. It is used to differentiate the local device from the neighbor device.
neighbor port	Port that connects the neighbor device to the local device.
unidirection detect information	Unidirectional link detection information.
bidirection detect information	Bidirectional link detection information.
loop detect information	Loop detection information.
action	Handling policy after a link exception is detected.
state	RLDP detection state of the port: ● **error**: Indicates that the link is abnormal. ● **normal**: Indicates that the link is normal.

The following example displays the RLDP state information of port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show rldp interface gigabitethernet 0/1
port state     : normal
local bridge   : 00d0.f822.37da
neighbor bridge : 00d0.f823.37db
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
    action: shutdown-port
    state : normal
```

```
bidirection detect information:
    action: shutdown-port
    state : normal
loop detect information:
    action: shutdown-port
    state : normal
```

Table 1-2 Output Fields of the show rldp interface Command

Field	Description
port state	Current state of the port: ● **Normal**: Indicates the normal state. ● **Error**: Indicates the failed state.
local bridge	MAC address of the local system. It is used to differentiate the local device from the neighbor device.
neighbor bridge	MAC address of the neighbor system. It is used to differentiate the local device from the neighbor device.
action	Handling policy after a link exception is detected.
state	RLDP detection state of the port: ● **error**: Indicates that the link is abnormal. ● **normal**: Indicates that the link is normal.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 rldp detect-latency

Function

Run the **rldp detect-latency** command to configure the loop detection latency interval of RLDP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default loop detection latency interval of RLDP is **0** seconds.

Syntax

rldp detect-latency *interval*

no rldp detect-latency

default rldp detect-latency

Parameter Description

interval: Loop detection latency interval of RLDP, in seconds. The value range is from 0 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to suppress RLDP loop detection for core devices. Therefore, the selected latency interval is generally greater than the RLDP loop detection interval of the downlink aggregation device.

Examples

The following example sets the loop detection latency interval of RLDP to 2 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rldp detect-latency 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 DLDP Commands

Command	Function
clear dldp	Clear statistics on the link up/down counts of a Data Link Detection Protocol (DLDP) monitoring point.
dldp	Enable the DLDP detection function.
dldp passive	Set the DLDP detection mode of a port to passive mode.
dldp interval	Configure a global detection interval for DLDP detection.
dldp retry	Configure the number of global retransmission times for DLDP detection.
dldp resume	Configure the number of link recovery times for all the DLDP detection operations.
show dldp	Display the configuration or statistics of DLDP monitoring points.

1.1 clear dldp

Function

Run the **clear dldp** command to clear statistics on the link up/down counts of a Data Link Detection Protocol (DLDP) monitoring point.

Syntax

clear dldp [**interface** *interface-type interface-number* [*ipv4-address*]]

Parameter Description

interface *interface-type interface-number*: Configures the interface type and interface number.

ipv4-address: IP address of the peer device.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

DLDP records the statistics on link up/down counts. You can run this command to clear the statistics on link up/down counts of a specified monitoring point and restart counting.

You can specify an L3 port or device IP address to clear the statistics of all the monitoring points or a monitoring point on the specified L3 port. When no parameter is specified, the statistics of all the monitoring points are cleared.

Examples

The following example clears statistics on the link up/down counts of each DLDP monitoring point.

```
Hostname> enable
Hostname# clear dldp
```

The following example clears statistics on the link up/down counts of all the monitoring points on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear dldp interface gigabitethernet 0/1
```

The following example clears statistics on the up/down counts of the link to 192.168.0.1 on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear dldp interface gigabitethernet 0/1 192.168.0.1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.2 dldp

Function

Run the **dldp** command to enable the DLDP detection function.

Run the **no** form of this command to disable this feature.

By default, the number of retransmission times of DLDP detection is **4**, the number of recovery times is **3**, and the detection interval is **1** second.

Syntax

dldp *ipv4-address* [*next-hop-ipv4-address*] [**mac-address** *mac-address*] [**interval** *tick-interval* | **resume** *resume-number* | **retry** *retry-number*]

no dldp *ipv4-address*

Parameter Description

ipv4-address: IP address of the peer device to be detected.

next-hop-ipv4-address: Next-hop IP address. If the peer device to be detected is in a different network segment, the next-hop IP address must be specified.

mac-address *mac-address*: Indicates the MAC address to be bound. If a next-hop IP address is specified, set this parameter to the MAC address of the next-hop device.

interval *tick-interval*: Configures the detection interval, in ticks (1 tick = 10 milliseconds). The value range is from 5 to 6000, and the value must be an integral multiple of 5.

resume *resume-number*: Configures the number of times for link recovery of the peer device to be detected, namely, the number of DLDP detection packets that need to be received consecutively before the link state changes from down to up. The value range is from 1 to 200.

retry *retry-number*: Configures the number of retransmission times. The value range is from 1 to 3600.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to enable DLDP detection, to rapidly detect an Ethernet link failure.

DLDP can detect multiple IP addresses configured on an L3 port. DLDP sets the port to down when none of the IP addresses returns an ICMP reply. If one of the IP addresses resumes communication, DLDP sets the port to up.

Examples

The following example sets the IP address of port GigabitEthernet 0/1 to 192.168.0.1/24, enables DLDP detection on this port, and sets the IP address of the peer device to be detected to 192.168.0.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# no switchport
Hostname(config-if-GigabitEthernet0/1)# ip address 192.168.0.1 255.255.255.0
Hostname(config-if-GigabitEthernet0/1)# dldp 192.168.0.2
```

The following example sets the IP address of port GigabitEthernet 0/1 to 192.168.0.1/24, enables inter-network segment DLDP detection on this port, and sets the IP address of the peer device to be detected to 192.168.1.1 and the next-hop routing IP address to 192.168.0.2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# no switchport
Hostname(config-if-GigabitEthernet0/1)# ip address 192.168.0.1 255.255.255.0
Hostname(config-if-GigabitEthernet0/1)# dldp 192.168.1.1 192.168.0.2
```

The following example disables DLDP detection for the peer IP address 192.168.0.2 on the port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# no dldp 192.168.0.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dldp interval**
- **dldp retry**
- **dldp resume**

1.3 dldp passive

Function

Run the **dldp passive** command to set the DLDP detection mode of a port to passive mode.

Run the **no** form of this command to remove this configuration.

The default DLDP detection mode is active mode.

Syntax

dldp passive

no dldp passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If DLDP detection is enabled on the devices at both ends and both devices send ICMP echo packets to each other to realize connectivity detection, duplicate packets will exist. During DLDP detection, so long as the device at one end sends an ICMP echo packet and the peer device judges whether the packet can be received in time by using the same detection parameters, both devices can detect the link connectivity. In this way, DLDP detection saves bandwidth and CPU resources. Therefore, the device responsible for sending ICMP echo packets can be configured to work in active mode, and the device used for only receiving ICMP echo packets can be configured to work in passive mode.

When the passive mode is enabled, ensure that the time parameter configuration of the peer device is completely consistent with that of the local device so that the link detection state is synchronized. Otherwise, in the passive mode, the link state may be misjudged because the peer device fails to send packets synchronously.

Examples

The following example sets the DLDP detection mode to passive mode for port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# dldp passive
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dldp**

1.4 dldp interval

Function

Run the **dldp interval** command to configure a global detection interval for DLDP detection.

Run the **no** form of this command to remove this configuration.

The default global detection interval of DLDP detection is **1** second.

Syntax

dldp interval *tick-interval*

no dldp interval

Parameter Description

tick- interval: Detection interval, in ticks (1 tick = 10 milliseconds). The value range is from 5 to 6000, and the value must be an integral multiple of 5.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configuration of this command takes effect immediately for all DLDP detection operations.

When a network device does not receive any reply packet from the peer device within the period of the detection interval multiplied by the number of detection retransmission times, the device determines that the L3 port is down (despite the physical link reachable). When normal communication is resumed, the L3 port is up.

When adjusting this parameter, you need to take into account the number of DLDP sessions and the CPP bandwidth; otherwise the device performance is consumed, and misjudgment and network flapping can be caused easily. Generally, you are advised to use the default configuration. When the number of DLDP sessions exceeds 10, you are advised to configure a detection interval not less than 100 ticks.

Examples

The following example sets a global detection interval of DLDP detection to 200 milliseconds (200 ticks).

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dldp interval 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 dldp retry

Function

Run the **dldp retry** command to configure the number of global retransmission times for DLDP detection.

Run the **no** form of this command to remove this configuration.

The default number of global retransmission times of DLDP detection is **4**.

Syntax

dldp retry *retry-number*

no dldp retry

Parameter Description

retry-number: Number of retransmission times. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configuration of this command takes effect immediately for all DLDP detection operations.

Setting the number of retransmission times to 1 can easily lead to misjudgment and network flapping. You are advised to set the number of retransmission times to 2 at least.

Examples

The following example sets the number of retransmission times to 4 for all DLDP detection operations.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dldp retry 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 dldp resume

Function

Run the **dldp resume** command to configure the number of link recovery times for all the DLDP detection operations.

Run the **no** form of this command to restore the default configuration.

The default number of link recovery times of all DLDP detection operations is **3**.

Syntax

dldp resume *resume-number*

no dldp resume

Parameter Description

no dldp resume: Configures the number of times for link recovery for the peer device to be detected. This parameter specifies the number of DLDP detection packets that need to be received consecutively before the link state changes from down to up. The value range is 1 to 200.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configuration of this command takes effect immediately for all DLDP detection operations.

Setting the number of recovery times to 1 can easily lead to misjudgment and network flapping. You are advised to set the number of recovery times to 2 at least.

Examples

The following example sets the number of link recovery times to 4 for all DLDP detection operations.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dldp resume 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show dldp

Function

Run the **show dldp** command to display the configuration or statistics of DLDP monitoring points.

Syntax

show dldp [**interface** *interface-type interface-number*] [**statistic**]

Parameter Description

interface *interface-type interface-number*: Configures the port type and number. If this parameter is not configured in the command, the related information of all ports is displayed.

statistic: Displays the statistics of DLDP monitoring points. If this parameter is not configured in the command, the configuration is displayed.

Defaults

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

You can specify parameters of an L3 port to display the configuration and statistics of all the monitoring points on the port.

Examples

The following example displays the configuration of all the monitoring points of DLDP.

```
Hostname> enable
Hostname# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
Gi0/1      Active   192.168.0.1  192.168.1.2  100       4      3      Up
Gi0/2      Passive  192.168.2.1             100       4      3      Up
```

The following example displays the configuration of all the monitoring points on L3 port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show dldp intface gigabitethernet 0/1
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
Gi0/1      Active   192.168.0.1  192.168.1.2  100       4      3      Up
```

Table 1-1 Output Fields of the show dldp Command

Field	Description
Interface	Name of a detected port.

Field	Description
Type	Detection mode.
Ip	IP address of the detected peer device.
Next-hop	Next-hop IP address for detection.
Interval	Detection interval.
Retry	Number of retransmission times.
Resume	Number of link recovery times.
State	Detection state.

The following example displays the statistics of all the monitoring points of DLDP.

```
Hostname> enable
Hostname# show dldp statistic
Interface  Type        Ip      record-time  Up-count  Down-count
Gi0/1     Active   192.168.0.1  2h34m5s     10       9
Gi0/2     Passive  192.168.2.1  1d2h3m52s    6        8
```

The following example displays the statistics of all the monitoring points on L3 port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show dldp interface gigabitethernet 0/1 statistic
Interface  Type        Ip      record-time  Up-count  Down-count
Gi0/1     Active   192.168.0.1  2h34m5s     10       9
```

Table 1-2 Output Fields of the show dldp statistic Command

Field	Description
Interface	Name of a detected port.
Type	Detection mode.
Ip	IP address of the detected peer device.
record-time	Time duration for collecting statistics on link up/down counts. The format of the displayed time duration is *y***d**h**m**s, where "y" indicates year, "d" indicates day, "h" indicates hour, "m" indicates minute, and "s" indicates second. Based on the values of the **Up-count** and **Down-count** parameters, you can know about the link up and down counts in this duration.
Up-count	Number of times that the protocol state is up, recorded for the corresponding monitoring point.
Down-count	Number of times that the protocol state is down, recorded for the corresponding monitoring point.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 VRRP Commands

Command	Function
show vrrp	Display the information of a VRRP group.
show vrrp interface	Display the VRRP group information of a specified port.
show vrrp packet statistics	Display the statistics of VRRP packets.
vrrp ipv6 accept_mode	Enable the function of receiving packets whose destination addresses are the IPv6 address of a virtual router.
vrrp authentication	Enable the VRRP packet authentication function.
vrrp bfd (Global configuration mode)	Configure the global IPv4 VRRP bidirectional forwarding detection (BFD).
vrrp bfd (Interface configuration mode)	Configure BFD correlation for an IPv4 VRRP group.
vrrp delay	Configure a startup delay for a VRRP backup group.
vrrp description	Configure a name for a VRRP group.
vrrp detection-vlan	Configure a method of sending IPv4 VRRP packets on a super VLAN port.
vrrp mode dual-active	Configure an IPv4 VRRP group to run in dual-active mode.
vrrp ip	Configure an IPv4 VRRP backup group and specify a virtual IPv4 address.
vrrp ipv6	Configure an IPv6 VRRP backup group and specify a virtual IPv6 address.
vrrp preempt	Configure the preemption mode for a VRRP group.
vrrp priority	Configure a priority for a VRRP group.
vrrp timers advertise	Configure the interval for the master device in a VRRP group to send VRRP advertisements.
vrrp timers learn	Enable the timer learning function for a VRRP group.
vrrp track	Enable the port link or IP route accessibility tracking function of IPv4 VRRP.

vrrp ipv6 track	Enable the port link or IP route accessibility tracking function of IPv6 VRRP.
vrrp version	Configure the standard for sending VRRP multicast packets for IPv4 VRRP.

1.1 show vrrp

Function

Run the **show vrrp** command to display the information of a VRRP group.

Syntax

show [**ipv6**] **vrrp** [**brief** | *group-id*]

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, the information of an IPv4 VRRP group is displayed.

brief: Displays brief information of VRRP. If this parameter is not specified, the complete information is displayed.

group-id: ID of a VRRP group. The value ranges from 1 to 255. If this parameter is not specified, the information of all VRRP groups is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified, the details of all IPv4 VRRP groups are displayed.

Examples

The following example displays the details of all the IPv4 VRRP groups.

```
Hostname> enable
Hostname# show vrrp
GigabitEthernet 0/1 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
GigabitEthernet 0/1 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
```

```
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
```

The following example displays the details of all the IPv6 VRRP groups.

```
Hostname> enable
Hostname# show ipv6 vrrp
GigabitEthernet 0/13 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::2
    1::2
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 1 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1 (local), priority is 100
  Master Advertisement interval is 1 sec
  Master Down interval is 3.60 sec
```

Table 1-1 Output Fields of the show vrrp Command

Field	Description
interface-type interface-number - Group *group-id*	• Backup group on a port. Here, *interface-type interface-number* indicates the type and number of the port, and *group-id* indicates the ID of the backup group.
State is *state*	The state of a VRRP group is *state*. Its value is as follows: • **Master**: Indicates the master state. • **Backup**: Indicates the backup state.
Virtual IP address is *ipv4-address* configured	Virtual IPv4 address of a backup group.
Virtual IPv6 address is as follows:*ipv6-address*	Virtual IPv6 address of a backup group.
Virtual MAC address is *mac-address*	Virtual MAC address of a backup group.
Advertisement interval is *interval* sec	The advertisement packet transmission interval is *interval* seconds.
Preemption is enabled	The preemption function of a backup group is enabled.

Field	Description
min delay is *min-delay* sec	The preemption delay of a backup group is *min-delay* seconds.
Priority is *priority*	The priority of a backup group is *priority*.
Master Router is *ipv4-address* (local), priority is *priority*	IP address and priority of a master router. Here, *ipv4-address* indicates an IPv4 address, and *priority* indicates a priority.
Master Advertisement interval is *interval* sec	The advertisement interval of a master router is *interval* second(s).
Master Down interval is *interval* sec	The interval for judging a failure of a master router is *interval* second(s).
Accept_Mode is enabled	The Accept_Mode of an IPv6 VRRP backup group is enabled.

The following example displays the brief information of all the IPv4 VRRP groups.

```
Hostname> enable
Hostname# show vrrp brief
Interface   Grp Pri timer   Own Pre State   Master addr     Group addr
Gi 0/1       1  100  10.82   -   P  Backup  192.168.201.213 192.168.201.1
Gi 0/1       2  120  10.59   -   P  Master  192.168.201.217 192.168.201.2
Hostname> enable
```

The following example displays the brief information of all the IPv6 VRRP groups.

```
Hostname# show ipv6 vrrp brief
Interface     Grp  Pri  timer  Own  Pre  State  Master addr  Group addr
Gi0/13        1    100  3.60   -    P    Master  FE80::1     FE80::2
```

Table 1-2 Output Fields of the show vrrp brief Command

Field	Description
Interface	Name of an Ethernet port.
Grp	ID of a VRRP backup group configured on a port.
Pri	Priority of a backup group.
timer	Interval for judging a failure of a master router, which is calculated by the backup group.
Own	Owner state of a backup group.
Pre	Preemption mode of a backup group.
State	State of a backup group.
Master addr	IP address of a master router.
Group addr	Primary virtual IP address of a backup group.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp interface**
- **show vrrp packet statistics**

1.2 show vrrp interface

Function

Run the **show vrrp interface** command to display the VRRP group information of a specified port.

Syntax

show [**ipv6**] **vrrp interface** *interface-type interface-number* [**brief**]

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, the information of an IPv4 VRRP group is displayed.

interface-type interface-number: Type and number of the port.

brief: Displays the brief information of a VRRP group. If this parameter is not specified, the details of a VRRP group are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified, the details of an IPv4 VRRP group are displayed.

Examples

The following example displays the details of an IPv4 VRRP group on the port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show vrrp interface gigabitethernet 0/1
GigabitEthernet 0/1 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
```

```
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
GigabitEthernet 0/1 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
```

Table 1-3 Output Fields of the show vrrp interface Command

Field	Description
interface-type interface-number - Group *group-id*	Backup group on a port. Here, *interface-type interface-number* indicates the type and number of the port, and *group-id* indicates the ID of the backup group.
State is *state*	The state of a VRRP group is *state*. Its value is as follows: ● **Master**: Indicates the master state. ● **Backup**: Indicates the backup state.
Virtual IP address is *ipv4-address* configured	Virtual IPv4 address of a backup group.
Virtual IPv6 address is as follows:*ipv6-address*	Virtual IPv6 address of a backup group.
Virtual MAC address is *mac-address*	Virtual MAC address of a backup group.
Advertisement interval is *interval* sec	The advertisement packet transmission interval is *interval* seconds.
Preemption is enabled	The preemption function of a backup group is enabled.
min delay is *min-delay* sec	The preemption delay of a backup group is *min-delay* seconds.
Priority is *priority*	The priority of a backup group is *priority*.
Master Router is *ipv4-address* (local), priority is *priority*	IP address and priority of a master router. Here, *ipv4-address* indicates an IPv4 address, and *priority* indicates a priority.

Field	Description
Master Advertisement interval is *interval* sec	The advertisement interval of a master router is *interval* second(s).
Master Down interval is *interval* sec	The interval for judging a failure of a master router is *interval* second(s).
Accept_Mode is enabled	The Accept_Mode of an IPv6 VRRP backup group is enabled.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp**
- **show vrrp packet statistics**

1.3 show vrrp packet statistics

Function

Run the **show vrrp packet statistics** command to display the statistics of VRRP packets.

Syntax

show vrrp packet statistics [*interface-type interface-number* | **total**]

Parameter Description

interface-type interface-number: Type and number of a port. If this parameter is not specified, the statistics of VRRP packets on all the ports are displayed.

total. Displays the total statistics of VRRP packets.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics of VRRP packets on all the ports.

```
Hostname> enable
Hostname# show vrrp packet statistics
Total
   InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826
   OutTransmits: 306079, OutOctets: 7798564
GigabitEthernet 0/1
   InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657
   OutTransmits: 272931, OutOctets: 6675320
GigabitEthernet 0/2
   InReceives: 0 packets, InOctets: 0, InErrors: 0
   OutTransmits: 681, OutOctets: 16344
```

The following example displays the statistics of VRRP packets on the port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show vrrp packet statistics gigabitethernet 0/1
GigabitEthernet 0/1
   InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657
   OutTransmits: 273053, OutOctets: 6677760
```

Table 1-4 Output Fields of the show vrrp packet statistics Command

Field	Description
Total	Statistics of VRRP packets on all the ports, including: ● Number of all the received VRRP packets. ● Number of bytes in all the received VRRP packets. ● Number of all the received VRRP error packets. ● Number of all the sent VRRP packets. ● Number of bytes in all the sent VRRP packets.
interface-type interface-number	Statistics of VRRP packets on a specific port, including: ● Number of the VRRP packets received by the port. ● Number of bytes in the VRRP packets received by the port. ● Number of VRRP error packets received by the port. ● Number of the VRRP packets sent by the port. ● Number of bytes in the VRRP packets sent by the port. *interface-type interface-number* indicates the port type and port number.
InReceives	Number of the received VRRP packets.
InOctets	Number of bytes in the received VRRP packets.
InErrors	Number of the received VRRP error packets.

Field	Description
OutTransmits	Number of the sent VRRP packets.
OutOctets	Number of bytes in the sent VRRP packets.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp**
- **show vrrp interface**

1.4 vrrp ipv6 accept_mode

Function

Run the **vrrp ipv6 accept_mode** command to enable the function of receiving packets whose destination addresses are the IPv6 address of a virtual router.

Run the **no** form of this command to disable this feature.

By default, an IPv6 VRRP group in the master state is not permitted to receive packets whose destination addresses are the IPv6 address of a virtual router, except the IPv6 VRRP group in owner state or the received NA/NS packets.

Syntax

vrrp ipv6 *group-id* **accept_mode**

no vrrp ipv6 *group-id* **accept_mode**

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on a network port and takes effect for a virtual router in master state.

You can configure this command for an IPv6 VRRP backup group only.

Examples

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, sets the ID of this IPv6 VRRP group to 1, and enables the function of receiving packets whose destination addresses are the IPv6 address of the virtual router on IPv6 VRRP group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 accept_mode
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp**

1.5 vrrp authentication

Function

Run the **vrrp authentication** command to enable the VRRP packet authentication function.

Run the **no** form of this command to disable this feature.

The VRRP packet authentication function is disabled by default, and no authentication password is configured.

Syntax

vrrp *group-id* **authentication** *authentication-string*

no vrrp *group-id* **authentication**

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

authentication-string: Authentication string for a VRRP group (it is a plaintext password of no more than eight bytes).

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The same authentication password must be configured for routers in the same VRRP group. The plaintext authentication password cannot guarantee security but only prevents or prompts wrong VRRP configurations. This command applies to VRRPv2 only.

Note

Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP). If VRRPv2 is selected for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1, sets the ID of this IPv4 VRRP group to 1, enables the VRRP packet authentication function on IPv4 VRRP group 1, and sets the authentication password to "x30dn78k".

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 authentication x30dn78k
```

Notifications

When the length of an entered authentication password exceeds eight bytes, the following notification will be displayed:

```
VRRP: Maximum authentication string length is 8.
```

Common Errors

- Different authentication modes are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.
- Plaintext password authentication is configured in a VRRP group, but the authentication strings are inconsistent, which results in multiple master routers in the group.

Platform Description

N/A

Related Commands

- **show vrrp**

1.6 vrrp bfd (Global configuration mode)

Function

Run the **vrrp bfd** command to configure the global IPv4 VRRP bidirectional forwarding detection (BFD).

Run the **no** form of this command to remove this configuration.

The global IPv4 VRRP BFD is not configured by default.

Syntax

vrrp bfd *interface-type interface-number ipv4-address*

no vrrp bfd

Parameter Description

interface-type interface-number: Type and number of a port.

ipv4-address: Neighbor IPv4 address to be detected by BFD.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Configuring global IPv4 VRRP BFD deletes the local correlation with BFD configured for all the single IPv4 VRRP groups.

If global IPv4 VRRP BFD is configured, reconfiguring it overwrites the old global BFD configuration, that is, the old global BFD configuration is deleted automatically.

For the port, on which BFD correlation needs to be configured, you need to configure the IP address and BFD session parameters first.

This command is only applicable to an IPv4 VRRP virtual router composed of two devices.

Examples

The following example configures global IPv4 VRRP BFD, detects the forwarding path between the master and backup routers of SVI 1 through BFD, and sets the neighbor IP address to be detected by BFD to 192.168.1.100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrrp bfd vlan 1 192.168.1.100
```

Notifications

When the specified BFD port is not an L3 port, the following notification will be displayed:

```
% Command is rejected because the interface should be a layer 3 interface.
```

When the specified IP address is not a valid IP address, the following notification will be displayed:

```
% Command is rejected because the IP address 127.0.0.1 is invalid.
```

When there is a separate BFD session in a VRRP backup group, the following notification will be displayed:

```
% All vrrp group bfd sessions were deleted because of global vrrp bfd was configured.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp ip**
- **vrrp bfd** (Interface configuration mode)

1.7 vrrp bfd (Interface configuration mode)

Function

Run the **vrrp bfd** command to configure BFD correlation for an IPv4 VRRP group.

Run the **no** form of this command to remove this configuration.

BFD correlation with an IPv4 VRRP group is not configured by default.

Syntax

vrrp *group-id* **bfd** *ipv4-address*

no vrrp *group-id* **bfd** *ipv4-address*

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

ipv4-address: Neighbor IPv4 address to be detected by BFD.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If global IPv4 VRRP BFD is configured, BFD correlation with an IPv4 VRRP group is not allowed on a port.

Before configuring this command, make sure that the IP address and BFD session parameters have been configured for a port, on which BFD correlation needs to be configured.

Examples

The following example adds SVI 1 of device 1 and SVI 1 of device 2 to VRRP group 1, sets the IP addresses of SVI 1 to 1.1.1.2 and 1.1.1.3 respectively, sets the virtual IP address of the VRRP group to 1.1.1.1, and configures BFD correlation with the master and backup routes for VRRP backup group 1.

The configuration on device 1 is as follows:

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip address 1.1.1.2 255.255.255.0
Hostname(config-if-VLAN 1)# bfd interval 50 min_rx 50 multiplier 3
Hostname(config-if-VLAN 1)# vrrp 1 ip 1.1.1.1
```

```
Hostname(config-if-VLAN 1)# vrrp 1 bfd 1.1.1.3
```

The configuration on device 2 is as follows:

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip address 1.1.1.3 255.255.255.0
Hostname(config-if-VLAN 1)# bfd interval 50 min_rx 50 multiplier 3
Hostname(config-if-VLAN 1)# vrrp 1 ip 1.1.1.1
Hostname(config-if-VLAN 1)# vrrp 1 bfd 1.1.1.2
```

Notifications

When the specified IP address is not a valid IP address, the following notification will be displayed:

```
VRRP: 127.0.0.1 is not a valid host address.
```

When there is a global IPv4 VRRP BFD session, the following notification will be displayed:

```
% Command is rejected because global vrrp bfd[vrrp bfd VLAN 1 1.1.1.2] configured.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bfd interval** (reliability/BFD)
- **vrrp ip**
- **vrrp bfd** (Global configuration mode)

1.8 vrrp delay

Function

Run the **vrrp delay** command to configure a startup delay for a VRRP backup group.

Run the **no** form of this command to remove this configuration.

No startup delay is configured for a VRRP backup group by default.

Syntax

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* } *

no vrrp delay

Parameter Description

minimum *min-seconds*: Configures a startup delay for a VRRP backup group when a port changes to the active state, in seconds. The value range is from 0 to 60, and the default value is **0**.

reload *reload-seconds*: Configures a startup delay for a VRRP backup group when the system is started, in seconds. The value range is from 0 to 60, and the default value is **0**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After a startup delay is configured for a VRRP group on a port, the VRRP backup group starts after the delay instead of starting immediately upon system startup or change of the port to the active state, to ensure that the non-preemption configuration takes effect. If the port receives a VRRP packet during the delay, the delay is canceled and VRRP is started immediately. This command configured on a network port is effective for both IPv4 VRRP and IPv6 VRRP.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, and sets the IP address of the port to 10.0.1.2, the VRRP group ID to 1, the virtual IP address to 10.0.1.1, the VRRP group startup delay after system startup to 10 seconds, and the VRRP group startup delay when the port changes to the active state to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp delay minimum 10 reload 10
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.2 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 vrrp description

Function

Run the **vrrp description** command to configure a name for a VRRP group.

Run the **no** form of this command to remove this configuration.

No VRRP group name is configured by default.

Syntax

vrrp [**ipv6**] *group-id* **description** *group-name*

no vrrp [**ipv6**] *group-id* **description**

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, a name is configured for an IPv4 VRRP group.

group-id: ID of a VRRP group. The value ranges from 1 to 255.

group-name: Name of the VRRP group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configuring a name for each VRRP group helps distinguish different VRRP groups.

Examples

The following example enables IPv4 VRRP on the port GigabitEthernet 0/1, and sets the group ID to 1 and group name to "BuildingA#", enables IPv6 VRRP on the port GigabitEthernet 0/2, and sets the group ID to 2 and group name to "BuildingB#".

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.2 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 description BuildingA#
Hostname(config-if-GigabitEthernet 0/1)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# vrrp 2 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 2 description BuildingB#
```

Notifications

When the length of a configured VRRP group name exceeds 80 bytes, the following notification will be displayed:

```
% The length of description is up to 80!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 vrrp detection-vlan

Function

Run the **vrrp detection-vlan** command to configure a method of sending IPv4 VRRP packets on a super VLAN port.

Run the **no** form of this command to restore the default configuration.

The IPv4 VRRP packets on a super VLAN port are sent to the first up sub VLAN only by default.

Syntax

vrrp detection-vlan { **first-subvlan** | *subvlan-id* }

no vrrp detection-vlan

Parameter Description

first-subvlan: Sends IPv4 VRRP packets only to the first up sub VLAN in a super VLAN.

subvlan-id: ID of a specified sub VLAN, to which IPv4 VRRP packets are sent. The value range is from 1 to 4094.

Command Modes

VLAN interface configuration mode

Default Level

14

Usage Guidelines

This command is configured on an SVI and effective only to super VLAN ports.

IPv4 VRRP packets can be sent in a super VLAN in three ways. Packets are sent to the first up sub VLAN in the super VLAN, or to a specified sub VLAN in the super VLAN, or to all the sub VLANs in the super VLAN. If VRRP and VRRP plus are both enabled on a super VLAN port, VRRP packets are sent to all the up sub VLAN ports of the super VLAN port.

Examples

The following example configures super VLAN 10 to send IPv4 VRRP packets to sub VLAN 2 only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-10
Hostname(config-vlan-range)# interface vlan 10
Hostname(config-if-VLAN 10)# supervlan
Hostname(config-if-VLAN 10)# subvlan 2-9
Hostname(config-if-VLAN 10)# ip address 10.10.1.2 255.255.255.0
Hostname(config-if-VLAN 10)# vrrp 1 ip 10.10.1.1
Hostname(config-if-VLAN 10)# vrrp detection-vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp ip**

1.11 vrrp mode dual-active

Function

Run the **vrrp mode dual-active** command to configure an IPv4 VRRP group to run in dual-active mode.

Run the **no** form of this command to restore the default configuration.

An IPV4 VRRP group runs in the master/backup mode by default.

Syntax

vrrp mode dual-active

no vrrp mode

Parameter Description

N/A

Command Modes

VLAN interface configuration mode

Default Level

14

Usage Guidelines

Configure this command on an SVI.

This command is used to configure the running mode of a VRRP group on an SVI. When **vrrp mode dual-active** is configured, the backup group runs in dual-active mode, in which the VRRP devices at both ends are in the master state. After the **no vrrp mode** command is configured, the master/backup mode is restored.

Examples

The following example configures a VRRP group on SVI 2 to run in the dual-active mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 2
Hostname(config-vlan)# interface vlan 2
Hostname(config-if-VLAN 2)# vrrp mode dual-active
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 vrrp ip

Function

Run the **vrrp ip** command to configure an IPv4 VRRP backup group and specify a virtual IPv4 address.

Run the **no** form of this command to remove this configuration.

No IPv4 VRRP backup group is configured by default.

Syntax

vrrp *group-id* **ip** *ipv4-address* [**secondary**]

no vrrp *group-id* **ip** *ipv4-address* [**secondary**]

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

ipv4-address: Virtual IPv4 address of an IPv4 VRRP backup group.

secondary: Configures the secondary IPv4 address for the virtual IP address of an IPv4 VRRP backup group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **secondary** parameter is not specified, the configured IP address becomes the primary IP address of a VRRP backup group.

Examples

The following example enables the VRRP function on the port GigabitEthernet 0/1, and sets the ID of this VRRP group to 1, the primary IP address of the VRRP backup group to 10.0.1.20, and the secondary IP address to 10.0.2.20.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.2.1 255.255.255.0 secondary
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.2.20 secondary
```

Notifications

When the **no** form of this command is configured on a port but there is no backup group of the specified backup group ID on this port, the following notification will be displayed:

```
VRRP:there is not ipv4 group 1 on interface Vl10.
```

When the specified virtual IP address is not a valid IP address, the following notification will be displayed:

```
VRRP:127.0.0.1 is not a valid host address.
```

When a virtual IP address is configured on a port, the port is bound to the multi-protocol virtual routing and forwarding (VRF) instance, but the VRF instance is not configured with an IPv4 address family, the following notification will be displayed:

```
VRRP: VLAN 10 is linked to a VRF. Enable IPv4 on that VRF first.
```

When the configured virtual IP address overlaps with the IP address of another port in the same VRF instance, the following notification will be displayed:

```
VRRP: 192.168.23.160 overlaps with other interface's address.
```

When the configured virtual IP address is a subnet address or broadcast address on the port, the following notification will be displayed:

```
VRRP: IP address 192.168.23.0 cannot be equal to interface broadcast or subnet address.
```

When a backup group is not configured with a primary virtual IP address but configured with a secondary virtual IP address directly, the following notification will be displayed:

```
VRRP: the first address assigned to IPv4 virtual router must be primary address!
```

When the **no** form of this command is configured to delete a secondary virtual IP address, but the secondary virtual IP address is not configured on the backup group, the following notification will be displayed:

```
VRRP: 192.168.23.162 is not secondary virtual IP address of ipv4 group 1 on interface
vl2.
```

When the **no** form of this command is configured to delete a primary virtual IP address but the primary virtual IP address is not configured on the backup group, the following notification will be displayed:

```
VRRP: 192.168.23.160 is not primary virtual IP address of ipv4 group 2 on interface
vl2.
```

When the **no** form of this command is configured to delete a primary virtual IP address but a secondary virtual IP address is configured on the backup group, the following notification will be displayed:

```
VRRP: all secondary addresses must be deleted before deleting primary address.
```

Common Errors

- Different virtual IP addresses are specified for the routers in the same VRRP backup group, resulting in multiple master routers in the group.

Platform Description

N/A

Related Commands

N/A

1.13 vrrp ipv6

Function

Run the **vrrp ipv6** command to configure an IPv6 VRRP backup group and specify a virtual IPv6 address.

Run the **no** form of this command to remove this configuration.

No IPv6 VRRP backup group is configured by default.

Syntax

vrrp *group-id* **ipv6** *ipv6-address*

no vrrp *group-id* **ipv6** *ipv6-address*

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

ipv6-address: Virtual IPv6 address of an IPv6 VRRP backup group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The IPv6 VRRP groups and IPv4 VRRP groups share the group ID range from 1 to 255. One VRRP backup group ID is applicable to an IPv4 VRRP backup group and an IPv6 VRRP backup group configured on the same port.

The first configured address must be a link local address, which can be deleted only after other virtual addresses are deleted.

Examples

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, and sets the ID of this VRRP group to 1 and the virtual IPv6 addresses to FE80::1 and 2001::1 respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)#ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2001::1
```

Notifications

When the **no** form of this command is configured on a port but there is no backup group of the specified backup group ID on this port, the following notification will be displayed:

```
VRRP:there is not ipv6 group 1 on interface vl2.
```

When the specified virtual IP address is not a valid IPv6 address, the following notification will be displayed:

```
VRRP:::1 is not a valid host address.
```

When a virtual IP address is configured on a port, the port is bound to a multi-protocol VRF instance, but the VRF instance is not configured with an IPv6 address family, the following notification will be displayed:

```
VRRP: VLAN 2 is linked to a VRF. Enable IPv6 on that VRF first.
```

When the configured virtual IP address overlaps with the IP address of another port in the same VRF instance, the following notification will be displayed:

```
VRRP: 2001::66 overlaps with other interface's address.
```

When the first virtual IP address configured for the backup group is not a link local address, the following notification will be displayed:

```
VRRP: the first address assigned to IPv6 virtual router must be link-local address.
```

When the **no** form of this command is configured to delete a virtual IP address, but the virtual IP address is not configured on the backup group, the following notification will be displayed:

```
VRRP: FE80::66 is not virtual IPv6 address of ipv6 group 1 on interface vl2.
```

When the **no** form of this command is configured to delete a link local address, but there is also a non-link local address, the following notification will be displayed:

```
VRRP: link-local address must be deleted at last.
```

Common Errors

- Different virtual IP addresses are specified for the routers in the same VRRP backup group, resulting in multiple master routers in the group.

Platform Description

N/A

Related Commands

N/A

1.14 vrrp preempt

Function

Run the **vrrp preempt** command to configure the preemption mode for a VRRP group.

Run the **no** form of this command to remove this configuration.

The VRRP backup group function is disabled by default. If the VRRP function is enabled, a VRRP backup group runs in preemption mode, and the master state is advertised without a delay.

Syntax

vrrp [**ipv6**] *group-id* **preempt** [**delay** *delay-seconds*]

no vrrp [**ipv6**] *group-id* **preempt** [**delay**]

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, this command configures the preemption mode for an IPv4 VRRP group.

group-id: ID of a VRRP group. The value ranges from 1 to 255.

delay-seconds: Delay time for advertising the master state, in seconds. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a VRRP group runs in preemption mode, a higher priority router takes the place of the lower priority master router. If a VRRP group runs in non-preemption mode, a router with a priority higher than that of the master router remains in backup state.

If the virtual IP address of a VRRP group is the same as the IP address of the port (in the owner state), the configured preemption mode is not effective, because the VRRP backup group of the port has the maximum priority 255, and automatically becomes the master device in the VRRP group.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, sets the ID of this IPv4 VRRP group to 1, and configures the router to preempt to become the master device after waiting for 15 seconds if the router judges that its priority (200) is higher than that of the current master device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 preempt delay 15
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 priority 200
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, sets the ID of this IPv6 VRRP group to 1, and configures the router to preempt to become the master device after waiting for 15 seconds if the router finds that its priority (200) is higher than that of the current master device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 preempt delay 15
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 priority 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp priority**

1.15 vrrp priority

Function

Run the **vrrp priority** command to configure a priority for a VRRP group.

Run the **no** form of this command to restore the default configuration.

The VRRP function is disabled by default. If the VRRP function is enabled, the priority of a VRRP group is 100.

Syntax

vrrp [**ipv6**] *group-id* **priority** *priority*

no vrrp [**ipv6**] *group-id* **priority**

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, this command configures the priority of an IPv4 VRRP group.

group-id: ID of a VRRP group. The value ranges from 1 to 255.

priority: Priority of a VRRP group. The value range is from 1 to 254.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, and sets the ID of this IPv4 VRRP group to **1** and the priority of IPv4 VRRP group 1 to **254**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 priority 254
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, and sets the ID of this IPv6 VRRP group to **1** and the priority of IPv6 VRRP group 1 to **254**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)#ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 254
```

Notifications

When the current backup group is in the owner state, the following notification will be displayed:

```
VRRP: Priority change will have no effect while interface is VRRP address owner.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp preempt**
- **vrrp track**

1.16 vrrp timers advertise

Function

Run the **vrrp timers advertise** command to configure the interval for the master device in a VRRP group to send VRRP advertisements.

Run the **no** form of this command to restore the default configuration.

The VRRP function is disabled by default. If the VRRP function is enabled, the interval for the master device to send advertisements is 1 second.

Syntax

vrrp [**ipv6**] *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

no vrrp [**ipv6**] *group-id* **timers advertise**

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, this command configures the interval for a device in an IPv4 VRRP group to send VRRP advertisements.

group-id: ID of a VRRP group. The value ranges from 1 to 255.

advertise-interval: Interval for sending VRRP advertisements, in seconds. The value range is from 1 to 255.

csec *centisecond-interval*: Specifies the interval for the master device in a backup group to send VRRP packets, in centiseconds. The value is an integer in the range from 50 to 99. No default value is provided. The command is only effective to VRRPv3 packets. If it is configured for VRRPv2, the default interval is **1** second for the master device.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the current device is elected as the master device in a VRRP group, it sends VRRP advertisement packets at the set interval to advertise its VRRP state, priority, and other information.

According to the RFC standard, the maximum interval for advertising multicast packets is **40** seconds. Therefore, if the advertisement interval configured is longer than 40 seconds, the maximum advertisement interval is applied, though the configuration is effective.

Examples

The following example enables the VRRP function on the port GigabitEthernet 0/1, and sets the ID of the backup group to 1 and the interval for sending IPv4 VRRP advertisements to 4 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 timers advertise 4
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, and sets the ID of the IPv6 VRRP group to 1 and the interval for sending IPv6 VRRP advertisements to 4 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 timers advertise 4
```

The following example enables the VRRP function on the port GigabitEthernet 0/1, and sets the ID of the backup group to 1 and the interval for sending IPv4 VRRP advertisements to 50 centiseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 version 3
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 timers advertise csec 50
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, and sets the ID of the IPv6 VRRP group to 1 and the interval for sending IPv6 VRRP advertisements to 50 centiseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 timers advertise csec 50
```

Notifications

When an IPv4 VRRP or IPv6 VRRP group is configured to adopt VRRPv3 for sending multicast packets, if the configured interval for sending advertisements exceeds 40 seconds, the following notification will be displayed:

```
VRRP: The Maximum adver time of VRRPv3 Packet is 40s.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp version**

1.17 vrrp timers learn

Function

Run the **vrrp timers learn** command to enable the timer learning function for a VRRP group.

Run the **no** form of this command to disable this feature.

The timer learning function of a VRRP group is disabled by default.

Syntax

vrrp [**ipv6**] *group-id* **timers learn**

no vrrp [**ipv6**] *group-id* **timers learn**

Parameter Description

ipv6: Indicates an IPv6 VRRP group. If this parameter is not specified, the timer learning function of an IPv4 VRRP group is enabled by default.

group-id: ID of a VRRP group. The value ranges from 1 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the timer learning function is enabled on a backup router, it learns the VRRP advertisement transmission interval from the master device and calculates the interval for determining the failure of the master device if no packet is received from the master device, instead of using the locally configured VRRP advertisement transmission interval for calculation.

This command achieves synchronization of the VRRP advertisement transmission timer between the master and backup routers.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, sets the ID of this IPv4 VRRP group to 1, and enables the timer learning function on IPv4 VRRP group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 timers learn
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, sets the ID of this IPv6 VRRP group to 1, and enables the timer learning function on IPv6 VRRP group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 timers learn
```

Notifications

N/A

Common Errors

- Different VRRP advertisement transmission intervals are configured in a VRRP group and the timer learning function is not configured, resulting in multiple master routers in the group.

Platform Description

N/A

Related Commands

- **vrrp timers advertise**

1.18 vrrp track

Function

Run the **vrrp track** command to enable the port link or IP route accessibility tracking function of IPv4 VRRP.

Run the **no** form of this command to disable this feature.

The IPv4 VRRP tracking function is disabled by default.

Syntax

vrrp *group-id* **track** { **bfd** *interface-type interface-number ipv4-address* | *interface-type interface-number* | *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] } [*Priority*]

no vrrp *group-id* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-address* | *ipv4-address* }

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

bfd *interface-type interface-number ipv4-address*: Tracks the neighbor IPv4 address of a specified port through BFD.

interface-type interface-number: Type and number of the monitored port.

ipv4-address: IPv4 address to be monitored.

interval *interval-value*: Configures the interval for sending detection packets, in seconds. The value range is from 1 to 3600. The default value is **3**.

timeout *timeout-value*: Configures the timeout time of waiting for a response to a sent detection packet, in seconds. If no response is received when the timeout time is up, it is determined that the destination is inaccessible once. The value range is from 1 to 60. The default value is **1**.

retry *retry-value*: Configures the number of retries. If no response is received for consecutive *retry-value* times, it is determined that the tracking status is inaccessible. The value range is from 1 to 60. The default value is **3**.

priority: VRRP priority change value when a monitored port link state or IP route accessibility state changes (for example, when the link is disconnected, the priority is reduced; when the link recovers, the priority is restored). The value range is from 1 to 255, and the default value is **10**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can use this command to monitor the egress link state and route accessibility state. A monitored port must be a routable L3 logical port (for example: a routed port, an SVI, a loopback port, or a tunnel port).

To monitor a host, specify its IPv4 address.

If a VRRP group uses the actual IP address of an Ethernet port, the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, sets the ID of this IPv4 VRRP group to 1, and configures VRRP group 1 to monitor GigabitEthernet 0/1. In this case, if the GigabitEthernet 0/1 link is disconnected, the priority of the VRRP group is reduced by 30; after the link of GigabitEthernet 0/1 is restored, the priority of VRRP group 1 is restored.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 priority 254
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 track GigabitEthernet 0/1 30
```

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, sets the ID of this IPv4 VRRP group to 1, configures VRRP group 1 to track the port GigabitEthernet0/1 through BFD, and sets the tracked neighbor IP address to 192.168.1.3. In this case, if the BFD tracking result is inaccessible, the priority of the VRRP group is reduced by 30; when the tracking result is accessible again, the priority of VRRP group 1 is restored.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
Hostname(config-if-GigabitEthernet 0/1)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.201.17 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 priority 120
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.201.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 track bfd gigabitethernet 0/1
192.168.1.3 30
```

Notifications

When the monitored port is not an L3 port, the following notification will be displayed:

```
VRRP: tracked interface must be a Layer 3 interface.
```

When the monitored IP address is not a valid IP address, the following notification will be displayed:

```
VRRP: 127.0.0.1 is not a valid host address.
```

When interval-value of the monitored address configured is smaller than timeout-value, the following notification will be displayed:

```
VRRP: interval must not be less than timeout.
```

When a specified VRRP group is configured to track a specified neighbor through BFD and the tracked port is not an L3 interface, the following notification will be displayed:

```
VRRP: tracked interface must be a Layer 3 interface.
```

When a specified VRRP group is configured to track a specified neighbor through BFD, but the neighbor address is not a valid address, the following notification will be displayed:

```
VRRP: 127.0.0.1 is not a valid host address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 vrrp ipv6 track

Function

Run the **vrrp ipv6 track** command to enable the port link or IP route accessibility tracking function of IPv6 VRRP.

Run the **no** form of this command to disable this feature.

The IPv6 VRRP tracking function is disabled by default.

Syntax

vrrp ipv6 *group-id* **track** { *interface-type interface-number* | { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] | **bfd** *interface-type interface-number peer-ipv6-address* } [*Priority*]

no vrrp ipv6 *group-id* **track** { *interface-type interface-number* | *ipv6-global-address* | *ipv6-linklocal-address interface-type interface- number* | **bfd** *interface-type interface-number peer-ipv6-address* }

Parameter Description

group-id: ID of a VRRP group. The value ranges from 1 to 255.

interface-type interface-number: Type and number of the monitored port.

ipv6-global-address: IPv6 global unicast address.

ipv6-linklocal-address: IPv6 link local address.

interval *interval-value*: Configures the interval for sending detection packets, in seconds. The value range is from 1 to 3600. The default value is **3**.

timeout *timeout-value*: Configures the timeout time of waiting for a response to a sent detection packet, in seconds. If no response is received when the timeout time is up, it is determined that the destination is inaccessible once. The value range is from 1 to 60. The default value is **1**.

retry *retry-value*: Configures the number of retries. If no response is received for consecutive *retry-value* times, it is determined that the tracking status is inaccessible. The value range is from 1 to 60. The default value is **3**.

priority: VRRP priority change value when a monitored port link state or IP route accessibility state changes (for example, when the link is disconnected, the priority is reduced; when the link recovers, the priority is restored). The value range is from 1 to 255, and the default value is **10**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can use this command to monitor the egress link state and route accessibility state. A monitored port must be a routable L3 logical port (for example: a routed port, an SVI, a loopback port, or a tunnel port).

To monitor a host, only specify its IPv6 address.

If a tracked host IP address is a link local address, specify a network port.

If a VRRP group uses the actual IP address of an Ethernet port, the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

Examples

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, sets the ID of this IPv6 VRRP group to 1, and configures VRRP group 1 to track whether the host 1000::1 is accessible. If it is inaccessible, the priority of the VRRP group is reduced to the default value **10**. After the accessibility recovers, the priority is restored.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 priority 254
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 track 1000::1
```

The following example enables the IPv6 VRRP function on the port GigabitEthernet 0/1 on a router, sets the ID of this IPv6 VRRP group to 1, configures VRRP group 1 to track whether the host FE80::2 on SVI 1 is accessible, and reduces the priority of the VRRP group to 20 when the host is accessible. After the accessibility recovers, the priority is restored.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 enable
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2001::1
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 priority 254
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 track fe80::2 vlan 1 20
```

Notifications

When the monitored port is not an L3 port, the following notification will be displayed:

```
VRRP: tracked interface must be a Layer 3 interface.
```

When the monitored IP address is not a valid IP address, the following notification will be displayed:

```
VRRP: 127.0.0.1 is not a valid host address.
```

When interval-value of the monitored address configured is smaller than timeout-value, the following notification will be displayed:

```
VRRP: interval must not be less than timeout.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 vrrp version

Function

Run the **vrrp version** command to configure the standard for sending VRRP multicast packets for IPv4 VRRP.

Run the **no** form of this command to restore the default configuration.

The default standard for sending IPv4 VRRP packets is VRRPv2 on a port.

Syntax

vrrp *group-id* **version** { **2** | **3** }

no vrrp *group-id* **version**

Parameter Description

group-id: ID of a VRRP group. The value range is from 1 to 255.

version 2: Uses the VRRPv2 standard to send multicast packets.

version 3: Uses the VRRPv3 standard to send multicast packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command applies to IPv4 VRRP only.

For IPv4 VRRP, to meet the requirements of the VRRPv2 and VRRPv3 switching scenario, you can specify a standard for sending VRRP packets based on the actual network condition. The VRRPv2 standard is based on RFC 3768, while the VRRPv3 standard is based on RFC 5798.

Examples

The following example enables the IPv4 VRRP function on the port GigabitEthernet 0/1 of a router, sets the ID of the IPv4 VRRP group to 1, and configures IPv4 VRRP group 1 to use VRRPv3 to send multicast packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.0.1.1 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 10.0.1.20
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 version 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrrp ip**

1 VRRP Plus Commands

Command	Function
show vrrp balance	Display the information of a Virtual Router Redundancy Protocol Plus (VRRP Plus) group.
show vrrp balance interface	Display the information of a VRRP Plus group on a specified interface.
vrrp balance	Enable the VRRP Plus function.
vrrp forwarder preempt	Enable the forwarding preemption function for a VRRP Plus backup group.
vrrp load-balancing	Configure a load balancing policy for a VRRP Plus group.
vrrp timers redirect	Configure the redirection interval and timeout time for a proxy virtual MAC address of a VRRP Plus backup group.
vrrp weighting	Configure the weight and upper and lower thresholds for a VRRP Plus backup group.
vrrp weighting track	Configure the track object for adjusting the weight for a VRRP Plus backup group.

1.1 show vrrp balance

Function

Run the **show vrrp balance** command to display the information of a Virtual Router Redundancy Protocol Plus (VRRP Plus) group.

Syntax

show [**ipv6**] **vrrp balance** [**brief** | *group-id*]

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the information of an IPv4 VRRP Plus group is displayed.

brief: Displays brief information of a VRRP Plus group. If this parameter is not specified, the detailed information of a VRRP Plus group is displayed.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If no parameter is specified, the detailed information of all the VRRP Plus groups is displayed.

Examples

The following example displays the detailed information of all the IPv4 VRRP Plus groups.

```
Hostname> enable
Hostname# show vrrp balance
VLAN 1 - Group-id 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1, upper 100
    Track object 1, state: down, decrement weight: 10
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
```

```
Owner ID is 00d0.f822.8800
```

The following example displays the detailed information of all the IPv6 VRRP Plus groups.

```
Hostname> enable
Hostname# show ipv6 vrrp balance
VLAN 2 - Group-id 1
  State is BVG
  Virtual IPv6 address is as follows:
    FE80::8
    2000::8
  Hello time 2 sec, hold time 6 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0201
    Owner ID is 00d0.f822.33f5
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2
    MAC address:
      1414.4b72.7701
    Owner ID is 00d0.f822.33b9
Preemption enabled
```

Table 1-1 Output Fields of the show vrrp balance Command

Field	Description
interface-type interface-number - Group *group-id*	Backup group on a port. Here, *interface-type interface-number* indicates the type and number of the port, and *group-id* indicates the ID of the backup group.
State is *role*	The role of the device in VRRP Plus is *role*, which can be set to the following values: ● **BVG**: Indicates the balancing virtual gateway. ● **BVF**: Indicates a balancing virtual forwarder.
Virtual IP address is *ipv4-address*	The virtual IPv4 address of the VRRP Plus group is *ipv4-address*.
Virtual IPv6 address is as follows: *ipv6-address*	The virtual IPv6 address of the IPv6 VRRP Plus group is *ipv6-address*.
Hello time *hello-time* sec	The interval at which the BVG sends keepalive packets is *hello-time* seconds.
hold time *hold-time* sec	The waiting time for a device to switch from the BVF role to the BVG role is *hold-time* seconds.

Field	Description
Load balancing:*loading-policy*	The type of the load balancing policy enabled on the VRRP Plus group is *loading-policy*, which can be set to the following values: ● **host-dependent**: Indicates the host-dependent load balancing policy. ● *round-robin*: Indicates the round-robin policy. ● *weighted*: Indicates the weighted policy.
Redirect time *redirect-time* sec, forwarder time-out *time-out* sec	Redirection time and timeout time of a proxy virtual MAC address. Here, *redirect-time* indicates the redirection time; and *time-out* indicates the timeout time.
Weighting *weight* (configured *configured-weight*), thresholds: lower *lower-threshold*, upper *upper-threshold*	Current weight, configured weight, upper threshold for weight, and lower threshold for weight of the device. Here, *weight* indicates the current weight; *configured-weight* indicates the configured weight; *upper-threshold* indicates the upper threshold for weight; and *lower-threshold* indicates the lower threshold for weight.
Track object *object*, state: *state*, decrement weight: *decrement-weight*	Object tracked by the track module and its state, as well as the weight decrement when the state is down. Here, *object* indicates the object tracked by the track module; *state* indicates the current state; and *decrement-weight* indicates the weight decrement when the state is down.
Forwarder *forwarder-number*	Forwarder of the VRRP Plus group. Here, *forwarder-number* indicates the forwarder number.
MAC addresss:*mac-address*	The virtual MAC address allocated to the device by the BVG is *mac-address*.
Owner ID is:*mac-address*	The real MAC address of the device is *mac-address*.
Preemption enabled	The forwarding preemption function is enabled for the VRRP Plus backup group.

The following example displays the brief information of a VRRP Plus group.

```
Hostname> enable
Hostname# show vrrp balance brief
Interface     Grp   State     Group-id Addr      MAC addr
VLAN 1         1    BVG       192.168.1.1        0000.5e00.0101
```

The following example displays the brief information of all the IPv6 VRRP Plus groups.

```
Hostname> enable
Hostname# show ipv6 vrrp balance brief
Interface            Grp   State     Group-id Addr       MAC addr
VLAN 2               1     BVG       FE80::8             0000.5e00.0201
```

Table 1-2 Output Fields of the show vrrp balance brief Command

Field	Description
Interface	Interface with VRRP Plus enabled.
Grp	ID of a VRRP group.
State	Role of the device in the VRRP Plus group, which can be set to the following values: ● **BVG**: Indicates the balancing virtual gateway. ● **BVF**: Indicates a balancing virtual forwarder.
Group-id Addr	Virtual IP address of the VRRP group.
MAC addr	Virtual MAC address of the device.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance interface**

1.2 show vrrp balance interface

Function

Run the **show vrrp balance interface** command to display the information of a VRRP Plus group on a specified interface.

Syntax

show [**ipv6**] **vrrp balance interface** *interface-type interface-number* [**brief**]

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the information of an IPv4 VRRP Plus group is displayed.

interface-type interface-number: Type and number of the port.

brief: Displays brief information of a VRRP Plus group. If this parameter is not specified, the detailed information of a VRRP Plus group is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the detailed information of an IPv4 VRRP Plus group on the Ethernet port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show vrrp balance interface gigabitethernet 0/1
GigabitEthernet 0/1 - Group-id 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1, upper 100
    Track object 1, state: down, decrement weight: 10
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
Owner ID is 00d0.f822.8800
```

The following example displays the detailed information of an IPv6 VRRP Plus group on the Ethernet port GigabitEthernet 0/2.

```
Hostname> enable
Hostname# show ipv6 vrrp balance interface gigabitethernet 0/2
GigabitEthernet 0/2 - Group-id 1
  State is BVG
  Virtual IPv6 address is as follows:
    FE80::8
    2000::8
  Hello time 1 sec, hold time 3 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0201
```

```
   Owner ID is 00d0.f822.33f5
   Preemption disabled (BVG cannot be preempted)
 Forwarder 2
   MAC address:
     1414.4b72.7701
   Owner ID is 00d0.f822.33b9
Preemption enabled
```

Table 1-3 Output Fields of the show vrrp balance interface Command

Field	Description
interface-type interface-number - Group *group-id*	Backup group on a port. Here, *interface-type interface-number* indicates the type and number of the port, and *group-id* indicates the ID of the backup group.
State is *role*	The role of the device in VRRP Plus is *role*, which can be set to the following values: **BVG**: Indicates the balancing virtual gateway. **BVF**: Indicates a balancing virtual forwarder.
Virtual IP address is *ipv4-address*	The virtual IPv4 address of the VRRP Plus group is *ipv4-address*.
Virtual IPv6 address is as follows: *ipv6-address*	The virtual IPv6 address of the IPv6 VRRP Plus group is *ipv6-address*.
Hello time *hello-time* sec	The interval at which the BVG sends keepalive packets is *hello-time* seconds.
hold time *hold-time* sec	The waiting time for a device to switch from the BVF role to the BVG role is *hold-time* seconds.
Load balancing:*loading-policy*	The type of the load balancing policy enabled on the VRRP Plus group is *loading-policy*, which can be set to the following values: ● **host-dependent**: Indicates the host-dependent load balancing policy. ● *round-robin*: Indicates the round-robin policy. ● *weighted*: Indicates the weighted policy.
Redirect time *redirect-time* sec, forwarder time-out *time-out* sec	Redirection time and timeout time of a proxy virtual MAC address. Here, *redirect-time* indicates the redirection time; and *time-out* indicates the timeout.
Weighting *weight* (configured *configured-weight*), thresholds: lower *lower-threshold*, upper *upper-threshold*	Current weight, configured weight, upper threshold for weight, and lower threshold for weight of the device. Here, *weight* indicates the current weight; *configured-weight* indicates the configured weight; *upper-threshold* indicates the upper threshold for weight; and *lower-threshold* indicates the lower threshold for weight.

Field	Description
Track object *object*, state: *state*, decrement weight: *decrement-weight*	Object tracked by the track module and its state, as well as the weight decrement when the state is down. Here, *object* indicates the object tracked by the track module; *state* indicates the current state; and *decrement-weight* indicates the weight decrement when the state is down.
Forwarder *forwarder-number*	Forwarder of the VRRP Plus group. Here, *forwarder-number* indicates the forwarder number.
MAC addresss:*mac-address*	The virtual MAC address allocated to the device by the BVG is *mac-address*.
Owner ID is:*mac-address*	The real MAC address of the device is *mac-address*.
Preemption enabled	The forwarding preemption function is enabled for the VRRP Plus backup group.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**

1.3 vrrp balance

Function

Run the **vrrp balance** command to enable the VRRP Plus function.

Run the **no** form of this command to disable this feature.

The VRRP Plus function is disabled by default.

Syntax

vrrp [**ipv6**] *group-id* **balance**

no vrrp [**ipv6**] *group-id* **balance**

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, an IPv4 VRRP Plus group is configured.

group-id: ID of a VRRP group. The value of the parameter ranges from 1 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To enable the VRRP Plus function, you need to first configured a VRRP group.

Examples

The following example enables the VRRP Plus function on the L3 port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
```

The following example enables the IPv6 VRRP Plus function on the L3 port GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 1 balance
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1.4 vrrp forwarder preempt

Function

Run the **vrrp forwarder preempt** command to enable the forwarding preemption function for a VRRP Plus backup group.

Run the **no** form of this command to disable this feature.

The forwarding preemption function is enabled for a VRRP Plus backup group by default.

Syntax

vrrp [**ipv6**] *group-id* **forwarder preempt**

no vrrp [**ipv6**] *group-id* **forwarder preempt**

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the forwarding preemption function is enabled for an IPv4 VRRP Plus group.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the forwarding preemption function for a VRRP Plus group on the L3 port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 forwarder preempt
```

The following example enables the forwarding preemption function for an IPv6 VRRP Plus backup group on the L3 port GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 1 balance
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 1 forwarder preempt
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1.5 vrrp load-balancing

Function

Run the **vrrp load-balancing** command to configure a load balancing policy for a VRRP Plus group.

Run the **no** form of this command to remove this configuration.

The default load balancing policy of a VRRP Plus group is round robin mode.

Syntax

vrrp [**ipv6**] *group-id* **load-balancing** { **host-dependent** | **round-robin** | **weighted** }

no vrrp [**ipv6**] *group-id* **load-balancing** { **host-dependent** | **round-robin** | **weighted** }

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the load balancing policy is configured for an IPv4 VRRP Plus group.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

host-dependent: Indicates the host-dependent load balancing policy. In this policy, different virtual MAC addresses are used to respond to ARP requests from different hosts.

round-robin: Indicates the round-robin load balancing policy. In this policy, different virtual MAC addresses are used to respond to host ARP requests in turn.

weighted: Indicates the weighted load balancing policy. In this policy, ARP replies are given based on weight values of devices in a backup group.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the host-dependent load balancing policy for VRRP Plus group 1 on the L3 port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 load-balancing host-dependent
```

The following example configures the host-dependent load balancing policy for IPv6 VRRP Plus group 1 on the L3 port GigabitEthernet 0/2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 1 balance
Hostname(config-if-GigabitEthernet 0/2)# vrrp ipv6 1 load-balancing host-dependent
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1.6 vrrp timers redirect

Function

Run the **vrrp timers redirect** command to configure the redirection interval and timeout time for a proxy virtual MAC address of a VRRP Plus backup group.

Run the **no** form of this command to restore the default configuration.

The default redirection interval of proxy virtual MAC addresses of a VRRP Plus backup group is **300** seconds and the default redirection timeout time is **14400** seconds.

Syntax

vrrp [**ipv6**] *group-id* **timers redirect** *redirect-interval redirect-timeout*

no vrrp [**ipv6**] *group-id* **timers redirect**

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the redirection interval and redirection timeout time are configured for a proxy virtual MAC address of an IPv4 VRRP Plus group.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

redirect-interval: Redirection interval, in seconds. The value range is from 0 to 3600.

redirect-timeout: Redirection timeout, in seconds. The value range is from (*redirect-interval*+600) to 64800.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You must enable the VRRP Plus function before configuring the redirection interval and timeout time for a proxy virtual MAC address of a VRRP Plus backup group.

Examples

The following example sets the redirection interval for a proxy virtual MAC address of VRRP Plus group 1 to **300** seconds and the redirection timeout time to **6000** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 timers redirect 300 6000
```

The following example sets the redirection interval for a proxy virtual MAC address of IPv6 VRRP Plus group 1 to **300** seconds and the redirection timeout time to **6000** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 timers redirect 300 6000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1.7 vrrp weighting

Function

Run the **vrrp weighting** command to configure the weight and upper and lower thresholds for a VRRP Plus backup group.

Run the **no** form of this command to restore the default configuration.

The default weight, default upper threshold, and default lower threshold of a VRRP Plus backup group are **100**, **1**, and **100** respectively.

Syntax

vrrp [**ipv6**] *group-id* **weighting** *weight-limit* [**lower** *min-weight-value*] [**upper** *max-weight-value*]

no vrrp [**ipv6**] *group-id* **weighting**

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the weight and upper and lower thresholds are configured for an IPv4 VRRP Plus group.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

weight-limit: Weight value. The value range is from 2 to 254.

lower *min-weight-value*: Indicates the lower threshold of the weight. The value range is from 1 to (*weight-limit* - 1).

upper *max-weight-value*: Indicates the upper threshold of the weight. The value range is from *min-weight-value* to *weight-limit.* That is, the value is between the minimum value of the weight (*min-weight-value*) and the maximum value of the weight (*weight-limit*).

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You must enable the VRRP Plus function before configuring the weight and upper and lower thresholds for a VRRP Plus backup group.

Examples

The following example sets the weight of VRRP Plus group 1 to **50**, and the lower threshold and upper threshold of weight to **30** and **50** respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 weighting 50 lower 30 upper 50
```

The following example sets the weight of IPv6 VRRP Plus 1 to **50**, and the lower threshold and upper threshold of weight to **30** and **50** respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 weighting 50 lower 30 upper 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1.8 vrrp weighting track

Function

Run the **vrrp weighting track** command to configure the track object for adjusting the weight for a VRRP Plus backup group.

Run the **no** form of this command to restore the default configuration.

This command is not configured by default.

Syntax

vrrp [**ipv6**] *group-id* **weighting track** *object-number* [**decrement** *value*]

no vrrp [**ipv6**] *group-id* **weighting track** *object-number*

Parameter Description

ipv6: Indicates an IPv6 VRRP Plus group. If this parameter is not specified, the track object for adjusting the weight is configured for an IPv4 VRRP Plus group.

group-id: ID of a VRRP Plus group. The value range is from 1 to 255.

object-number: Number of the track object created by the track module. The value range is from 1 to 700.

value: Weight decrement when the track object is down. The value range is from 1 to 255. The default value is **10**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the track object for adjusting the weight for VRRP Plus group 1, configures the group to track the port GigabitEthernet 0/2, and sets the weight decrement when the track object is down to 50.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 1 interface gigabitethernet 0/2 line-protocol
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.1.1
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 weighting track 1 decrement 50
```

The following example configures the track object for adjusting the weight for IPv6 VRRP Plus group 1, configures the group to track the port GigabitEthernet 0/2, and sets the weight decrement when the track object is down to 50.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 1 interface gigabitethernet 0/2 line-protocol
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 address 2000::1/64
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 fe80::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp 1 ipv6 2000::8
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 balance
Hostname(config-if-GigabitEthernet 0/1)# vrrp ipv6 1 weighting track 1 decrement 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show vrrp balance**
- **show vrrp balance interface**

1 BFD Commands

Command	Function
bfd interval	Configure bidirectional forwarding detection (BFD) session parameters.
bfd bind peer-ip	Associate the interface status with the BFD sessions status.
bfd cpp	Enable BFD protection.
bfd echo	Enable the echo mode.
bfd slow-timer	Configure the slow timer time in the echo mode.
bfd up-dampening	Configure a delay for status change advertisement, after which BFD informs an associated application.
sbfd reflector discriminator	Configure a seamless bidirectional forwarding detection (SBFD) reflector discriminator.
show bfd neighbors	Display the information of a BFD session.
show sbfd reflector discriminator	Display the information of an SBFD reflector discriminator.
show sbfd reflector initiator-mapping	Display the mappings between the SBFD reflector and the initiator.

1.1 bfd interval

Function

Run the **bfd interval** command to configure bidirectional forwarding detection (BFD) session parameters.

Run the **no** form of this command to remove this configuration.

Bidirectional forwarding detection (BFD) session parameters are not configured by default..

Syntax

bfd interval *send-interval* **min_rx** *receive-interval* **multiplier** *multiplier-value*

no bfd interval

Parameter Description

interval *send-interval*: Configures the interval of sending BFD control packets to a neighbor of a BFD session, which is also the interval of echo packets. The value ranges from 50 to 999, in milliseconds.

min_rx *receive-interval*: Configures the interval for the local device of a BFD session to receive BFD control packets from a neighbor. The value ranges from 50 to 999, in milliseconds.

multiplier-value: Maximum number of BFD control packets from the peer end that can be discarded within the negotiation interval. The value range is from 3 to 50.

Command Modes

Interface configuration mode

BFD template configuration mode

Default Level

14

Usage Guidelines

You are advised to keep the parameter configuration consistent at both ends of a BFD session. The purpose is to ensure that the application protocols associated with BFD take effect simultaneously and prevent occurrence of one-way forwarding path due to different dampening time at both ends.

Transmission bandwidth differences of different interfaces need to be taken into account during parameter configuration. If the configured minimum Tx interval and minimum Rx interval are very small, BFD may occupy excessive bandwidth and affect data transmission.

When a session negotiation is not completed on a port during command execution, the system prompts that a session negotiation is in progress and returns a configuration failure.

Examples

The following example configures the BFD session parameters for the L3 port GigabitEthernet0/1, and sets the interval of sending BFD packets to **100** ms, the interval of receiving BFD packets to **100** ms, and the maximum number of packets that can be discarded to **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet0/1)# bfd interval 100 min_rx 100 multiplier 3
```

The following example configures the BFD session parameters for the template template1, and sets the interval of sending BFD packets to **100** ms, the interval of receiving BFD packets to **100** ms, and the maximum number of packets that can be discarded to **3**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bfd-template multi-hop template1
Hostname(config-bfd)# bfd interval 100 min_rx 100 multiplier 3
```

Notifications

When the memory is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough memory for this config.
```

When the interface line bandwidth is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough bandwidth for this config.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 bfd bind peer-ip

Function

Run the **bfd bind peer-ip** command to associate the interface status with the BFD sessions status.

Run the **no** form of this command to remove this configuration.

No interface status is associated with the BFD sessions status by default.

Syntax

bfd bind peer-ip *ipv4-address* [**source-ip** *ipv4-address*] **process-pst**

no bfd bind peer-ip *ipv4-address*

Parameter Description

peer-ip *ipv4-address*: Configures the peer IP address for detection. It must be set to the address of a directly connected L3 interface.

source-ip *ipv4-address*: Configures the source IP address for sending BFD packets. The source IP address is specified to ensure that packets are not discarded by the unicast reverse path forwarding (URPF) when BFD is used together with URPF and other functions. The default source IP address is **0**, and the source IP address is learned through BFD session negotiation.

process-pst: Associates the session with the BFD state of an L3 interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configure this command on an L3 interface and make sure that the detected peer IP address is the address of the directly connected interface.

Examples

The following example enables BFD on the L3 port GigabitEthernet 0/1, and sets the peer IP address to 192.168.0.2, and associates the interface with the BFD state of the interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# ip address 192.168.0.1 255.255.255.0
Hostname(config-if-GigabitEthernet0/1)# bfd bind peer-ip 192.168.0.2 source-ip
192.168.0.1 process-pst
```

Notifications

When the memory is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough memory for this config.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 bfd cpp

Function

Run the **bfd cpp** command to enable BFD protection.

Run the **no** form of this command to disable this feature.

BFD protection is enabled by default.

Syntax

bfd cpp

no bfd cpp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The BFD protocol is very sensitive. If a BFD-enabled device is attacked, BFD protection can be enabled to provide protection.

If both BFD and BFD protection are enabled, the device discards the BFD packets received from the previous-hop device, which affects the establishment of a BFD session between the previous-hop device and other devices.

Examples

The following example enables BFD protection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bfd cpp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 bfd echo

Function

Run the **bfd echo** command to enable the echo mode.

Run the **no** form of this command to disable this feature.

The echo mode is disabled for a BFD session by default.

Syntax

bfd echo [**one-arm**]

no bfd echo

Parameter Description

one-arm: Indicates a one-armed echo mode.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By default, when BFD session parameters are configured, the system automatically enables the asynchronous mode, and disables the one-armed echo mode.

The minimum TX interval and minimum RX interval of echo packets adopt the **Interval** *send-interval* and **min_rx** *receive-interval* parameters of a session.

Before enabling the echo mode or one-armed echo mode of BFD, run the **no ip redirects** command on the neighbors of a BFD session to disable the function of sending ICMP redirection packets, and run the **no ip deny land** command to disable the distributed denial of service (DDoS) function to prevent the land-based attack.

The echo mode takes effect only after it is enabled at both ends of a BFD session.

The one-armed echo mode takes effect when it is enabled at one end of a BFD session.

In the process that the forwarding plane of the peer device returns echo packets transmitted by the local end to the local end, the echo packets may be lost due to congestion of the peer device, causing a session detection failure. In this case, you need to configure a quality of service (QoS) policy to ensure that echo packets are processed preferentially or disable the echo function.

Examples

The following example enables the echo mode on the L3 port GigabitEthernet0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# bfd echo
```

The following example enables the one-armed echo mode on the L3 port GigabitEthernet0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet0/1)# bfd echo one-arm
```

Notifications

When the memory is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough memory for this config.
```

When the interface line bandwidth is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough bandwidth for this config.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 bfd slow-timer

Function

Run the **bfd slow-timer** command to configure the slow timer time in the echo mode.

Run the **no** form of this command to restore the default configuration.

The default slow timer time in the echo mode is **2000** milliseconds.

Syntax

bfd slow-timer [*interval*]

no bfd slow-timer

Parameter Description

interval: Slow timer time of BFD, in milliseconds. The value range is from 1000 to 30000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the slow timer time in the echo mode to **14000** milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bfd slow-timer 14000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 bfd up-dampening

Function

Run the **bfd up-dampening** command to configure a delay for status change advertisement, after which BFD informs an associated application.

Run the **no** form of this command to restore the default configuration.

The default delay for status change advertisement, after which BFD informs an associated application of BFD up is **0** seconds.

Syntax

bfd up-dampening *interval*

no bfd up-dampening

Parameter Description

interval: Required delay for status change advertisement, after which BFD informs an associated application of BFD up, in milliseconds. The value range is 0 to 300000. When the parameter is set to **0**, the associated application is informed immediately when the session state is switched from down to up.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Enable this function only when the link is unstable.

If a BFD session does not frequently switch between the down and up states, configuring this command will delay notifying an associated application of BFD up.

Examples

The following example sets the delay for status change advertisement, after which BFD informs an associated application of BFD up, to **60,000** milliseconds on the port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

```
Hostname(config-if-GigabitEthernet0/1)# bfd up-dampening 60000
```

Notifications

When the memory is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough memory for this config.
```

When the interface line bandwidth is insufficient during the execution of this command and the configuration fails, the following notification will be displayed:

```
no enough bandwidth for this config.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 sbfd reflector discriminator

Function

Run the **sbfd reflector discriminator** command to configure a seamless bidirectional forwarding detection (SBFD) reflector discriminator.

Run the **no** form of this command to remove this configuration.

No SBFD reflector discriminator is configured by default.

Syntax

sbfd reflector discriminator { *unsigned-integer-descriptor* | *ipv4-address* }

no sbfd reflector discriminator { *unsigned-integer-descriptor* | *ipv4-address* }

Parameter Description

unsigned-integer-descriptor: Discriminator of the integer type. The value range is from 16777216 to 4294967295.

ipv4-address: IPv4 address, in dotted decimal notation.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Like BFD sessions, SBFD sessions also distinguish different sessions through My Discriminator and Your Discriminator. Since the reflector of SBFD does not perceive the detection service and is responsible for only

looping back packets, only a reflector discriminator needs to be configured by running the **reflector discriminator** command at the reflector. This discriminator is Your Discriminator for the initiator.

In a network, one initiator can be deployed to map to multiple reflectors, and multiple reflector discriminators can be configured for one reflector. All the reflector discriminators in the network must be globally unique.

Examples

The following example sets the SBFD reflector discriminator to 16777216.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sbfd reflector discriminator 16777216
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show sbfd reflector discriminator**

1.8 show bfd neighbors

Function

Run the **show bfd neighbors** command to display the information of a BFD session.

Syntax

show bfd neighbors [**vrf** *vrf-name*] [**client** { **ap** | **bgp** | **isis** | **ospf** | **ospfv3** | **rip** | **vrrp** | **static-route** | **pbr** | **vrrp-balance** | **bgp-lsp** | **ldp-lsp** | **static-lsp** | **backward-lsp-with-ip** | **pst** | **dhcp** | **openflow** | **pimdm** | **pimsm** | **pimsmv6** | **srp** }] [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*] [**details**] [**parm-consult** [*interface-type interface-number*]]

Parameter Description

vrf *vrf-name*: Specifies the name of a virtual routing forwarding (VRF) instance, to which a neighbor belongs. The global VRF instance is displayed by default.

client: Displays a specified application protocol. All the application protocols are displayed by default.

ap: Displays the information of a BFD session associated with an L3 aggregate port (AP) member port.

bgp: Displays the information of a BFD session associated with Border Gateway Protocol (BGP).

isis: Displays the information of a BFD session associated with Intermediate System to Intermediate System (IS-IS).

ospf: Displays the information of a BFD session associated with Open Shortest Path First (OSPF).

ospfv3: Displays the information of a BFD session associated with OSPFv3.

rip: Displays the information of a BFD session associated with Routing Information Protocol (RIP).

vrrp: Displays the information of a BFD session associated with Virtual Router Redundancy Protocol (VRRP).

static-route: Displays the information of a BFD session associated with static routing.

pbr: Displays the information of a BFD session associated with policy-based routing (PBR).

vrrp-balance: Displays the information of a BFD session associated with VRRP Plus.

bgp-lsp: Displays the information of a BFD session associated with BGP label switched paths (LSPs).

ldp-lsp: Displays the information of a BFD session associated with Label Distribution Protocol (LDP) LSPs.

backward-lsp-with-ip: Displays the information of a BFD session associated with IP addresses of reverse LSPs.

static-lsp: Displays the information of a BFD session associated with static LSPs.

pst: Displays the information of a BFD session associated with an L3 interface.

dhcp: Displays the information of a BFD session associated with Dynamic Host Configuration Protocol (DHCP).

openflow: Displays the information of a BFD session associated with open flow.

pimdm: Displays the information of a BFD session associated with Protocol Independent Multicast-Dense Mode (PIM-DM).

pimsm: Displays the information of a BFD session associated with Protocol Independent Multicast-Sparse Mode (PIM-SM).

pimsm: Displays the information of a BFD session associated with PIM-SMv6.

srp: Displays the information of a BFD session associated with SRP.

ipv4 *ipv4-address*: Displays the information of a specific IPv4 session. The information of all the sessions is displayed by default.

ipv6 *ipv6-address*: Displays the session information of a specific IPv6 neighbor. The information of all the sessions is displayed by default.

details: Displays the details. The brief information is displayed by default.

parm-consult: Displays the number of BFD sessions that have completed negotiation.

parm-consult *interface-type interface-number*: Displays the number of BFD sessions that have completed negotiation on a specified port.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

In the information displayed by running the **show bfd neighbors** command, "OurAddr" indicates the source address of a session. When it is displayed as "-", no source address is specified. For example, the command is run on a BFD session associated with IP addresses of reverse LSPs. "Int" indicates the interface information of a session. When it is displayed as "-", no interface is specified. For example, the command is run on a session

associated with a protocol that does not carry interface information, and the system prompt logs of the session do not contain the interface information.

Examples

The following example displays the basic information of BFD sessions.

```
Hostname> enable
Hostname# show bfd neighbors
IPV4 sessions: 1, UP: 1
IPV6 sessions: 0, UP: 0
OurAddr       NeighAddr     LD/RD      RH/RS    Holdown(mult)  State  Int
192.168.24.2   192.168.24.1   8192/8192    Up     0(3   )       Up
GigabitEthernet 0/1
```

The following example displays the details of BFD sessions.

```
Hostname> enable
Hostname# sh bfd neighbors details
IPV4 sessions: 1, UP: 1
IPV6 sessions: 0, UP: 0
OurAddr       NeighAddr     LD/RD      RH/RS    Holdown(mult)  State  Int
192.168.24.2   192.168.24.1   8192/8192    Up     0(3   )       Up
GigabitEthernet 0/1
Session state is Up and using echo function with 50 ms interval.
Local Diag:   0,       Demand mode:   0,      Poll bit:   0
MinTxInt: 3000000,         MinRxInt: 3000000,          Multiplier:   3
Received MinRxInt 3000000, Multiplier: 3
Holdown (hits): 9000(0), Hello (hits): 3000(36)
Rx Count: 127, Rx Interval (ms) min/max/avg: 40/999/999
Tx Count: 135, Tx Interval (ms) min/max/avg: 1000/1000/999
Registered protocols: VRRP
Uptime: 0:01:19
Last packet:
 Version         :        1               - Diagnostic    : 0
 State bit       :       Up               - Demand bit    : 0
 Poll bit        :        0               - Final bit     : 0
 Multplier       :        3               - Length        : 24
 My Discr        :     8192               - Your Discr    : 8192
 Min tx interval  :   3000000               - Min rx interval: 3000000
 Min Echo interval:    50000
```

The following example displays the information about a BFD session associated with the L3 AP application.

```
Hostname> enable
Hostname# show bfd neighbors client ap
IPV4 sessions: 1, UP: 0
IPV6 sessions: 0, UP: 0
OurAddr       NeighAddr      LD/RD     RH/RS   Holdown(mult) State  Int
192.168.23.1   192.168.23.2    8192/0    Admin    0(3   )      Down   GigabitEthernet
0/2 (AP 1)
```

The following example displays the number of BFD sessions that have completed negotiation.

```
Hostname> enable
Hostname# show bfd neighbors parm-consult
IPV4 sessions: 1, UP: 1  consult-Finish: 1
IPV6 sessions: 0, UP: 0  consult-Finish: 0
OurAddr       NeighAddr      LD/RD     RH/RS   Holdown(mult) State  Int
192.168.23.1   192.168.23.2    8192/8192  UP     0(3   )      UP    GigabitEthernet
0/2 (AP 1)
```

Table 1-1 Output Fields of the show bfd neighbors Command

Field	Description
IPV4 sessions	Total number of IPv4 BFD sessions and number of up sessions.
IPV6 sessions	Total number of IPv6 BFD sessions and number of up sessions.
OurAddr	Local IP address of a session.
NeighAddr	Neighbor IP address of the session.
LD/RD	Local and remote discriminators of the session.
RH/RS	Current state of the session's peer end.
Holdown(mult)	Time when the local end of the session fails to receive hello packets and number of session detection timeout times.
State	Current state of the session.
Int	ID of the interface where the session is.
Session state is UP and using echo function with 50 ms interval	Whether the session is in the echo mode and the time interval of sending echo packets (the information is displayed only in the echo mode).
Local Diag	Diagnostic information of the session.
Demand mode	Whether the session query mode is activated.
Poll bit	Whether the configuration of the session is modified.
MinTxInt	Minimum Tx interval configured at the local end of the session.
MinRxInt	Minimum Rx interval configured at the local end of the session.
Multiplier	Number of detection timeout times configured at the local end of the session.
Received MinRxInt	Minimum Tx interval configured at the remote end of the session.
Received Multiplier	Number of detection timeout times configured at the remote end of the session.

Field	Description
Holdown (hits)	Session detection time and the number of detected timeout times.
Hello (hits)	Minimum interval of receiving hello packets after session negotiation.
Rx Count	Number of BFD packets received by the local end of the session.
Rx Interval (ms) min/max/avg	Minimum interval, maximum interval, and average interval of receiving packets at the local end of the session.
Tx Count	Number of BFD packets sent at the local end of the session.
Tx Interval (ms) min/max/avg	Minimum interval, maximum interval, and average interval of transmitting packets at the local end of the session.
Registered protocols	Type of the application protocol registered to the session.
Uptime	Up time of the session.
Last packet	Information of the last BFD packet received at the local end of the session.
consult-Finish	Statistics of the sessions that have completed negotiation.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show sbfd reflector discriminator

Function

Run the **show sbfd reflector discriminator** command to display the information of an SBFD reflector discriminator.

Syntax

show sbfd reflector discriminator

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

To display the reflector information of SBFD, run the **show sbfd reflector discriminator** command.

Examples

The following example displays the information of an SBFD reflector discriminator.

```
Hostname> enable
Hostname# show sbfd reflector discriminator
Reflec-Discr(INT)    Reflec-Discr(IP)             State          CreateType
16777216             1.0.0.0                     Active         Integer
Total Discriminator Num : 1
```

Table 1-2 Output Fields of the show sbfd reflector discriminator Command

Field	Description
Reflec-Discr(INT)	SBFD reflector discriminator of the integer type.
Reflec-Discr(IP)	IP address of the SBFD reflector.
State	Status of the SBFD reflector.
CreateType	Character type of the SBFD reflector.
Total Discriminator Num	Number of SBFD reflector discriminators.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show sbfd reflector initiator-mapping

Function

Run the **show sbfd reflector initiator-mapping** command to display the mappings between the SBFD reflector and the initiator.

Syntax

show sbfd reflector initiator-mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

To display the information of the initiator associated with a reflector, run the **show sbfd reflector initiator-mapping** command.

Examples

The following example displays the mappings between the SBFD reflector and the initiator.

```
Hostname> enable
Hostname# show sbfd reflector initiator-mapping
Reflec-Discr        Initia-Discr        Int
16777216            10000               Gi1/0/5
16777216            10001               Gi1/0/5
16777216            10002               Gi1/0/5
16777216            10003               Gi1/0/6
16777216            10004               Gi1/0/6
16777216            10005               Gi1/0/6
Total Initiator-mapping Num : 6
```

Table 1-3 Output Fields of the show sbfd reflector initiator-mapping Command

Field	Description
Reflec-Discr	SBFD reflector discriminator of the integer type.
Initia -Discr	SBFD initiator discriminator of the integer type.
Int	Outbound interface of SBFD reflector response packets.
Total Initiator-mapping Num	Total number of mappings between the SBFD reflector and the initiator.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 Track Commands

Command	Function
delay	Configure the delay for notifying the status change of a track object.
dhcp	Create a reliable network service (RNS) test of Dynamic Host Configuration Protocol (DHCP) type.
dns	Create an RNS test of DNS type.
frequency	Configure a test interval.
icmp-echo	Create an RNS test of ICMP echo type.
ip rns	Define a track operation object.
ip rns reaction-configuration	Configure the proactive threshold monitoring and triggering mechanism for a test.
ip rns reaction-trigger	Trigger another test in pending state to activate when the monitoring threshold exceeds the expectation during a test.
ip rns reset	Clear the configurations of all tests.
ip rns restart	Restart a test.
ip rns schedule	Configure the scheduling policy of a test.
ip rns-server udp-echo	Configure the IP RNS server to provide server functions for the test of UDP echo type.
object	Configure a member object for a track list object.
request-data-size	Configure the protocol payload size of a test.
show ip rns-server	Display the configuration information of an RNS server object.
show ip rns configuration	Display the configuration information of a track object.
show ip rns collection-statistics	Display the detailed statistics of a test.
show ip rns operational-state	Display the current status of a test.
show ip rns reaction-configuration	Display the proactive threshold monitoring information of a test.

show ip rns reaction-trigger	Display the test trigger information of a test.
show ip rns statistics	Display the brief statistics of a track object.
show track	Display the statistics of a track object.
tag	Configure a tag for an IP test.
tcp-connect	Configure a TCP test.
threshold	Configure the upper threshold of a test.
timeout	Configure the timeout interval of a test.
tos	Configure the type of service (TOS) field in the IPv4 packet of a test.
track interface line-protocol	Configure a track object, which is used to track the link status of an interface.
track list	Configure a track object for tracking the status of a track list.
track rns	Configure a track object, which is used to track the test result of a track instance.
track rns-list	Configure a track object, which is used to track the test result of an rns-list instance.
udp-echo	Configure a test object of UDP echo type.
vrf	Configure the VRF of a test.

1.1 delay

Function

Run the **delay** command to configure the delay for notifying the status change of a track object.

Run the **no** form of this command to restore the default configuration.

No delay is set by default for notifying the track object status change from up to down or from down to up.

Syntax

delay { **up** *interval* [**down** *interval*] | **down** *interval* [**up** *interval*] }

no delay

Parameter Description

up *interval*: Specifies the delay for notifying the status change of a track object from down to up, in seconds. The value range is from 0 to 180.

down *interval*: Specifies the delay for notifying the status change of a track object from up to down, in seconds. The value range is from 0 to 180.

Command Modes

Track configuration mode

Default Level

1

Usage Guidelines

When the status of a track object frequently changes, the status of the client that uses the track object will frequently change as well.

Run this command to delay the notification of the status change of a track object. For example, if the status of a track object changes from up to down, and the **delay down** command is configured, the down status of the track object is notified 10s later. If the status of the track object changes to up again within this period of time, no notification is sent. Therefore, the status of the track object is always up on the client that uses this track object.

Examples

The following example configures track object 5 for tracking track instance 10. When the status of the track object changes from down to up, the notification is delayed for 30 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 5 rns 10
Hostname(config-track)# delay up 30
```

Notifications

When no track object is configured, the following notification will be displayed:

```
set delay error.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 dhcp

Function

Run the **dhcp** command to create a reliable network service (RNS) test of Dynamic Host Configuration Protocol (DHCP) type.

No RNS test of DHCP type is created by default.

Syntax

dhcp *destination-ipv4-address* **out-interface** *interface-type interface-number* **next-hop** *next-ipv4-address*

Parameter Description

destination-ipv4-address: Destination host IP address for testing.

out-interface interface-type interface-number: Specifies the outbound interface for test packets.

next-hop *next-ipv4-address*: Specifies the next hop IP address for test packets.

Command Modes

IP RNS configuration mode

Default Level

1

Usage Guidelines

The RNS test of DHCP type supports the IPv4 network only.

After an RNS test of DHCP type is started, the system sends a DHCP packet to test whether the network of the target host is connected, and whether the destination host has the function of DHCP service. After an RNS test of DHCP type is created, the system enters the IP RNS DHCP mode.

You need to configure the test type, such as Internet Control Message Protocol (ICMP) echo or domain name server (DNS), before configuring its specific parameters. To modify the type of a test instance, delete the instance by running the **no ip rns** command in global configuration mode.

Examples

The following example creates test instance 1 of DHCP type. The instance requests the DHCP service of 172.30.30.3 through the GigabitEthernet 0/1 interface and the next hop address 172.30.31.1.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# dhcp 172.30.30.3 out-interface GigabitEthernet 0/1 next-hop
172.30.31.1
Hostname(config-ip-rns-dhcp)#
```

Notifications

When you want to create a test of DHCP type, if the memory allocation fails, the configuration fails and the following notification will be displayed:

```
rns object rns-dhcp create fail
```

Common Errors

- When a test of DHCP type is created, the DHCP service is not enabled on the server.
- When a test of DHCP type is created, no IP address is configured for the outbound interface of the client.

Platform Description

N/A

Related Commands

N/A

1.3 dns

Function

Run the **dns** command to create an RNS test of DNS type.

No RNS test of DNS type is created by default.

Syntax

dns { **oob** *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] **via** *interface-type interface-number* **next-hop** *ipv4-address* } | { *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] [

[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]] }

dns *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]]

Parameter Description

oob: Indicates the test on the MGMT port.

destination-hostname: Destination host name. The maximum length is 127 characters, and the excess part is truncated automatically.

name-server *ipv4-address*: Indicates the IP address of the DNS server.

source-ipaddr *ipv4-address*: Indicates the source IP address.

out-interface *interface-type interface-number*: Specifies the outbound interface (not the MGMT port) for test packets.

af-direct: Indicates that packets are received and sent without passing through the protocol stack in the test.

via *interface-type interface-number*: Specifies the MGMT port as the egress interface for the test packets.

next-hop *ipv4-address*: Indicates the next hop IP address when the outbound interface is specified.

Command Modes

IP RNS configuration mode

Default Level

1

Usage Guidelines

The RNS test of DNS type supports the IPv4 network only.

After an RNS test of DNS type is started, the system sends a DNS parsing request packet to test whether the device is connected to the target host. After an RNS test of DNS type is created, the system enters the IP RNS DNS mode.

You need to configure the test type, such as Internet Control Message Protocol (ICMP) echo or domain name server (DNS), before configuring its specific parameters. To modify the type of a test instance, delete the instance by running the **no ip rns** command in global configuration mode.

Examples

The following example creates test instance 1 of DNS type. The DNS server address configured for this instance is 61.154.22.41, and the IP address of the domain name www.abc.com is requested.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# dns www.abc.com name-server 61.154.22.41
Hostname(config-ip-rns-dns)#
```

Notifications

When you want to create a test of DNS type, if the memory allocation fails, the configuration fails and the following notification will be displayed:

```
rns object dns create fail
```

Common Errors

- When you want to create a test of DNS type, the memory allocation fails.
- When you want to create a test of DNS type, the maximum length of the destination host name consists of 127 characters, and the excess part is truncated automatically.

Platform Description

N/A

Related Commands

N/A

1.4 frequency

Function

Run the **frequency** command to configure a test interval.

Run the **no** form of this command to remove this configuration.

The default test interval is **60** seconds.

Syntax

frequency *interval*

no frequency

Parameter Description

interval: Packet transmission interval, in milliseconds. The value range is from 10 to 604800000. The maximum duration is 1 week.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

In the lifetime of a test, the test is conducted periodically. Run the **frequency** command to specify the test interval. The configuration must comply with the following formula to ensure correct test calculation.

(**frequency** *interval*) > (**timeout** *interval*) ≥ (**threshold** *interval*)

Examples

The following example configures test instance 1 of ICMP echo type, and sets the test destination IP address of this instance to 192.168.21.1, the test frequency to 30 seconds, the timeout to 8000 milliseconds, and the threshold to 6000 milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 192.168.21.1
Hostname(config-ip-rns-icmp-echo)# frequency 30000
Hostname(config-ip-rns-icmp-echo)# timeout 8000
Hostname(config-ip-rns-icmp-echo)# threshold 6000
```

Notifications

When you configure a test repeat interval shorter than the timeout interval, the configuration fails and the following notification will be displayed:

```
Illegal Value: Cannot set Frequency to be less than Timeout
```

Common Errors

- The configured test repeat interval is shorter than the timeout interval.

Platform Description

N/A

Related Commands

N/A

1.5 icmp-echo

Function

Run the **icmp-echo** command to create an RNS test of ICMP echo type.

No RNS test of ICMP echo type is created by default.

Syntax

icmp-echo { **oob** { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address*] **via** *interface-type interface-number* **next-hop** *ipv4-address* } | { { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address* | **source-interface** *interface-type interface-number*] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]] }

icmp-echo { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address* | **source-interface** *interface-type interface-number*] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]]

Parameter Description

oob: Indicates the test on the MGMT port.

destination-ipv4-address: Destination IPv4 address.

Destination-hostname: Destination host name. The maximum length is 127 characters, and the excess part is truncated automatically.

name-server *ipv4-address*: Specifies the DNS server when the destination host name is configured. By default, the DNS server configured by running the **ip name-server** command is used for address resolution.

source-ipaddr *ipv4-address*: Indicates the source IPv4 address.

source-interface *interface-type interface-number*: Specifies the source interface type and number.

out-interface *interface-type interface-number*: Specifies the outbound interface (not the MGMT port) for test packets.

af-direct: Indicates that packets are received and sent without passing through the protocol stack in the test.

via *interface-type interface-number*: Specifies the MGMT port as the egress interface for the test packets.

next-hop *ipv4-address*: Indicates the next hop IPv4 address when the outbound interface is specified.

Command Modes

IP RNS configuration mode

Default Level

1

Usage Guidelines

After an ICMP echo test is started, the system sends an ICMP echo request packet to test whether the device is connected to the target host. After an ICMP echo test instance is created, the system enters the IP RNS ICMP echo mode. The default protocol payload size of an ICMP echo request packet is **36** bytes. Run the **request-data-size** command to change the packet size. You need to configure the test type, such as Internet Control Message Protocol (ICMP) echo or domain name server (DNS), before configuring its specific parameters. To modify the type of a test instance, delete the instance by running the **no ip rns** command in global configuration mode.

You are not advised to use the **name-server** parameter, but use **ip name-server** to configure a DNS.

Examples

The following example configures IP test instance 1 of ICMP echo type, and sets the destination IP address of this instance to 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)#
```

Notifications

When you want to create a test of ICMP echo type, if the memory allocation fails, the configuration fails and the following notification will be displayed:

```
rns object icmp-echo create fail.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

No test

1.6 ip rns

Function

Run the **ip rns** command to define a track operation object.

Run the **no** form of this command to remove this configuration.

No track operation object is created by default.

Syntax

ip rns *operation-number* [{ **dns** *destination-hostname* **name-server** *ipv4-address* | **icmp-echo** *destination-ipv4-address* | **tcp-connect** *destination-ipv4-address port-number* } [**frequency** *interval*] [**timeout** *interval*] [**threshold** *interval*]]

no ip rns *operation-number*

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500.

dns *destination-hostname* **name-server** *ipv4-address*: Briefly configures a DNS test.

destination-hostname: Destination host name. The maximum length is 127 characters, and the excess part is truncated automatically.

name-server *ipv4-address*: Indicates the IPv4 address of the DNS server.

icmp-echo *destination-ipv4-address*: Briefly configures an ICMP echo test.

destination-ipv4-address: Destination IPv4 address.

tcp-connect *destination-ipv4-address port-number*: Briefly configures a Transmission Control Protocol (TCP) connect test.

destination-ipv4-address: Destination IPv4 address.

port-number: TCP port to be tested.

frequency *interval*: Indicates the test repeat interval.

timeout *interval*: Configures the timeout interval of an IP test.

threshold *interval*: Configures the upper threshold of an IP test.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Currently, only IPv4-related tests are supported, but IPv6-related tests are not supported. At most 500 tests can be configured, depending on the performance of devices. The test function is only a value-added function. When a large number of tests are configured and consume a lot of system resources, the test function may be temporary disabled to ensure normal operation of core services, such as route forwarding.

Detailed configuration (executing mandatory items of **ip rns** *operation-number*): Run this command and enter the IP RNS mode. In this mode, you can define various test types. If the test type is not configured, the track object is not created. After configuring a test, you must run the **ip rns** *operation-number* command to configure its scheduling startup policy; otherwise, the test cannot be conducted.

After configuring the type of a test, you can run the **ip rns** command to enter the configuration mode of the corresponding test type. To modify the type of a test, you must first delete the test by running the **no ip rns** command in global configuration mode.

Brief configuration (executing the subsequent optional test items of **ip rns**): After optional items are executed, it is equivalent that **ip rns** *operation-number*, **ip rns schedule**, detailed test configuration (such as the ICMP

echo test), **frequency**, **timeout**, and **threshold** are executed according to the logical sequence. Among these commands, the **ip rns schedule** command is executed to start a test by using the *start-time now life forever* parameter. For details about restrictions of other configuration items, see the related description in the detailed configuration.

Similarly, to modify a briefly configured test, you need to first delete this test by running the **no ip rns** command in global configuration mode before re-configuration.

Examples

The following example defines test instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)#
```

The following example defines test instance 1 of ICMP echo type, and sets the test destination IP address of this instance to 10.1.1.1, the threshold to 10 seconds, the timeout interval to 20 seconds, and the test frequency to 30 seconds.

```
Hostname(config)# ip rns 1 icmp-echo 10.1.1.1 threshold 10000 timeout 20000 frequency
30000
```

Notifications

When you define a track operation object, if the operation object ID is already configured and the object is running, you will enter the IP RNS mode and the following notification will be displayed:

```
Entry already running and cannot be modified
(only can delete (no) and start over)
(check to see if the probe has finished exiting)
```

Common Errors

- When you run the **ip rns** command, if the corresponding test is already configured and is running, you cannot enter the mode corresponding to the test type. To modify the test configuration, you must first delete the scheduling configuration by running the **no ip rns schedule** command.

Platform Description

N/A

Related Commands

- **frequency**
- **threshold**
- **timeout**

1.7 ip rns reaction-configuration

Function

Run the **ip rns reaction-configuration** command to configure the proactive threshold monitoring and triggering mechanism for a test.

Run the **no** form of this command to remove this configuration.

The proactive threshold monitoring and triggering mechanism is not configured for the test by default.

Syntax

ip rns reaction-configuration *operation-number* **react** { **allfail** | **rtt** | **timeout** } [**action-type track**] [**threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] }] [**threshold-value** *max-threshold min-threshold*]

no ip rns reaction-configuration *operation-number* [**react** *monitored-element*]

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500.

react { **allfail** | **rtt** | **timeout** }: Specifies the monitored test information element (*monitored-element*). **allfail** indicates that monitoring all elements fails, and only correlation with track is supported. **rtt** indicates that the packet round trip time is not within the threshold range. **timeout** indicates timeout in either direction.

action-type { **track | trigger** }: Indicates the action taken after the test is triggered. Only correlation with trigger or track is supported. Correlation with the track action is allowed only when the monitored test information element is **allfail**. This parameter is not configured by default, namely, no action is taken.

average [*number-of-measurements*]: Indicates that the test is triggered if the average of number-of-measurements of the monitored element exceeds the threshold. For example, set the value of number-of-measurements to 3, upper threshold to 5000, and lower threshold to 4000. If the values of three consecutive tests are 6000, 6000, and 5000 respectively, their average is (6000 + 6000 + 5000)/3 = 5667, exceeding the upper threshold 5000. The value range of number-of-measures is from 1 to 16, and the default value is **5**.

consecutive [*occurrences*]: Indicates that the action is triggered if the number of consecutive occurrences of the monitored element exceeds the threshold. The value range of occurrences is from 1 to 16. The default value is **5**.

immediate: Indicates that the action is triggered immediately after the monitored element exceeds the threshold.

never: Indicates that the action is never triggered.

xofy [*x-value y-value*]: Indicates that results of X tests exceed the threshold in the last Y tests. The value ranges of both X and Y are from 1 to 16. The default values of X and Y are both **5**.

threshold-value *max-threshold min-threshold*: Indicates the upper and lower thresholds. When the monitored test information element is **rtt**, the thresholds indicate time, in milliseconds, and the value range is from 0 to 60000. For default values, see *Usage Guidelines*. When the monitored test information element is **timeout**, the **threshold-vaule** parameter does not need to be configured.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

You can configure multiple thresholds for one test to monitor different elements. The following table lists the mappings between test types and monitored elements.

Table 1-1 Mapping Table of Test Types and Monitored Elements

monitored-element	icmp-echo	dns	tcp-connect	udp-echo
timeout				
rtt				

The following table lists the default thresholds of each monitored element.

Table 1-2 Mapping Table of Monitored Elements and Default Thresholds

monitored element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000 ms	0 ms

Examples

The following example configures to trigger the action when the monitored element of test instance 1 times out in any direction and the timeout exceeds the threshold range, and supports correlation with trigger only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns reaction-configuration 1 react timeout threshold-type
immediate action-type trigger
```

Notifications

When you configure the proactive threshold for the test of a track instance, if creation of a react variable memory fails, the configuration will fail and the following notification will be displayed:

```
rns react malloc fail
```

When the configured information type of monitored test element is not supported, the configuration will fail and the following notification will be displayed:

```
rns entry %d detect not support this react_type %s [reacttype name]
```

Common Errors

- The configured information type of the monitored test element is not supported.

Platform Description

N/A

Related Commands

N/A

1.8 ip rns reaction-trigger

Function

Run the **ip rns reaction-trigger** command to trigger another test in pending state to activate when the monitoring threshold exceeds the expectation during a test.

Run the **no** form of this command to remove this configuration.

The trigger mechanism when the monitoring threshold exceeds the expectation is not configured for the test by default.

Syntax

ip rns reaction-trigger *source-operation-number target-operation-number*

no ip rns reaction-trigger *source-operation-number target-operation-number*

Parameter Description

source-operation-number: Number of the source operation triggering the action. The value range is from 1 to 500.

target-operation-number: Number of the triggered target operation. The value range is from 1 to 500.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

The trigger function is generally used in network fault diagnosis scenario. In a common scenario, you do not need to configure the trigger function.

Examples

The following example triggers to activate track instance 2 in pending state when the monitoring threshold of test instance 1 exceeds the expectation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns reaction-trigger 1 2
```

Notifications

When you configure a test trigger object, if the memory allocation for the trigger object fails, the configuration will fail and the following notification will be displayed:

```
rns trigger malloc fail
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip rns reset

Function

Run the **ip rns reset** command to clear the configurations of all tests.

Syntax

ip rns reset

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Run this command to clear all the track configurations. This command is used only in extreme cases, for example, when a lot of track tests are configured but the configurations are found incorrect.

Examples

The following example clears all the test configurations.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns reset
```

Notifications

The following notification will be displayed when you run **ip rns reset** to clear all the track configurations, and you need to confirm the operation. The default value is **no**.

```
WARNING: rns reset will remove all rns configurations, continue? (y/n) [no]
```

If a track instance is being tested, you will be prompted to confirm the deletion. The default value is **no**.

```
rns 1 schedule is running, confirm to delete?(y/n) [no]
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip rns restart

Function

Run the **ip rns restart** command to restart a test.

Syntax

ip rns restart *operation-number*

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

This command restarts an ip rns test for which the scheduling policy is configured and is in pending state of scheduling. This command is invalid for a test for which the scheduling policy is not configured.

Examples

The following example restarts test instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns restart 1
```

Notifications

If the specified test is not configured, the test will fail to restart and the following notification will be displayed:

```
rns operate has not define
```

If the specified test is not configured with rns schedule, the test will fail to restart and the following notification will be displayed:

```
% rns 2 schedule is not configured.
```

If the specified test is running, the test will fail to restart and the following notification will be displayed:

```
rns 1 schedule is active state.
```

Common Errors

- The specified test is not configured.
- The rns schedule configuration is not configured.
- The specified test is running.

Platform Description

N/A

Related Commands

N/A

1.11 ip rns schedule

Function

Run the **ip rns schedule** command to configure the scheduling policy of a test.

Run the **no** form of this command to remove this configuration.

No scheduling policy is configured for the test by default.

Syntax

ip rns schedule *operation-number* [**life** { **forever** | *period* }] [**start-time** { *hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss* }] [**recurring**]

no ip rns schedule *operation-number*

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500.

life forever: Indicates that the life of RNS operation is always valid.

life *period*: Indicates the life period of the ip rns test. That is, after the test starts at the configured start-time, the test stops in the time set for *period***.**

hh:*mm* [:*ss*]: Accurate operation start time, in a 24-hour system.

month: Month in which the operation starts. The default value is the current month. The format is the English abbreviation or full name of January to December.

day: Date on which the operation starts. The default value is the current day. The value range is from 1 to 31.

pending: Indicates that the start time of the operation is not defined, and the default value is used.

now: Indicates that the operation start time is now and the operation will start immediately.

after *hh*:*mm*:*ss*: Indicates that the operation starts after a delay of hh:mm:ss.

recurring: Indicates that the operation starts at the same time every day.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

If a test of scheduling policy has been configured by running the **ip rns schedule** command and the test has started, the test parameters cannot be modified. To modify the configuration, you need to first run the **no ip rns schedule** command to delete the scheduling configuration.

Examples

The following example configures to start test instance 1 immediately and makes it permanently valid.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns schedule 1 start-time now life forever
```

The following example makes the test unmodifiable after a scheduling policy is configured. The test can be modified after the scheduling policy is deleted.

```
Hostname(config)# ip rns 1
Entry already running and cannot be modified
       (only can delete (no) and start over)
       (check to see if the probe has finished exiting)
Hostname(config)# no ip rns schedule 1
Hostname(config)# ip rns 1
Hostname(config-ip-rns-icmp-echo)# exit
```

Notifications

When you configure the scheduling policy of a test, if memory allocation fails, configuration of the scheduling policy will fail and the following notification will be displayed:

```
ip rns malloc rns schedule fail
```

When the schedule object is already configured and being tested, the configuration will fail and the following notification will be displayed:

```
Cannot modify schedule. Operation may have started.
```

Common Errors

- The **ip rns schedule** object is already configured and running.

Platform Description

N/A

Related Commands

N/A

1.12 ip rns-server udp-echo

Function

Run the **ip rns-server udp-echo** command to configure the IP RNS server to provide server functions for the test of UDP echo type.

Run the **no** form of this command to remove this configuration.

The server for UDP echo test is not configured by default.

Syntax

ip rns-server udp-echo *port-number*

no ip rns-server udp-echo

Parameter Description

udp-echo: Configures the server for the UDP echo test.

port-number: Number of the port monitored by the UDP service on the RNS server. The value range is from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

If the RNS type is UDP echo, the RNS server must be enabled on the peer end to process the test packet.

Examples

The following example configures the IP RNS server to provide server functions for the UDP echo test, and configures the port for UDP service monitoring as 1025.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns-server udp-echo 1025
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 object

Function

Run the **object** command to configure a member object for a track list object.

Run the **no** form of this command to delete a track member.

No member object is configured by default.

Syntax

object *object-number* [**not**]

no object *object-number*

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700.

Command Modes

Track configuration mode

Default Level

1

Usage Guidelines

Run this command to configure a member object for a track list. The number of track list members that can be configured is restricted by the capacity of track objects only.

If the status of the track object is consistent with that of the member object, only when the member object is in the up status, can the track object be in the up status.

If the status of the track object is contrary to that of the member object, only when the member object is in the down status, can the track object be in the up status.

Configure this command only when the track object is in the track mode of list.

A track object cannot track itself.

Track objects cannot track each other. For example, if Track A tracks Track B, Track B cannot track Track A in reverse. Otherwise, the statuses of Track A and Track B may change frequently.

Examples

The following example configures track object 4. When the status of track object 1 is up, the status of track object 2 is down, and the status of track object 3 is up, track object 4 is up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 4 list boolean and
Hostname(config-track)# object 1
Hostname(config-track)# object 2 not
Hostname(config-track)# object 3
```

Notifications

When no track object is configured or the configuration fails, the following notification will be displayed if you configure this **object** command:

```
set object error.
```

If a configured member object is the track object itself, the configuration will fail and you will be prompted that the track object cannot track itself.

```
track can not track itself.
```

If the configured member object has tracked this track object, the configuration will fail and the following notification will be displayed:

```
object xx is already tracking track yy.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 request-data-size

Function

Run the **request-data-size** command to configure the protocol payload size of a test.

Run the **no** form of this command to restore the default configuration.

The default protocol payload sizes of both the ICMP echo test and UDP echo test are **36**.

Syntax

request-data-size *bytes*

no request-data-size

Parameter Description

bytes: Number of bytes in the payload of the test packet. The minimum/maximum bytes are different for respective tests. The value range of the ICMP echo test and the UDP echo test is from 36 to 1472.

Command Modes

IP RNS ICMP Echo configuration mode

IP RNS UDP Echo configuration mode

Default Level

1

Usage Guidelines

This command is used to stuff some bytes in the test packet so that large packets can be used for the test.

Examples

The following example configures test instance 1 of ICMP echo type, and sets the test destination address to 10.1.1.1 and the protocol load size to 50.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# request-data-size 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show ip rns-server

Function

Run the **show ip rns-server** command to display the configuration information of an RNS server object.

Syntax

show ip rns-sever udp-echo

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the configuration information of an RNS server object. The configuration information varies with packet types.

Examples

The following example displays the configuration information of ip rns-server udp.

```
Hostname> enable
Hostname# show ip rns-server udp-echo
   UDP-Echo-Server: 0.0.0.0:1026
   Receive packets number: 0
   Reflect packets success number: 0
Reflect packets fail number: 0
```

Table 1-3 Output Fields of the show ip rns-server udp-echo Command

Field	Description
UDP-Echo-Server	Server address of the UDP echo test, including the server IP address and port information
Receive packets number	Number of received packets
Reflect packets success number	Number of response packets that are sent successfully

Field	Description
Reflect packets fail number	Number of response packets that cannot be sent

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show ip rns configuration

Function

Run the **show ip rns configuration** command to display the configuration information of a track object.

Syntax

show ip rns configuration [*operation-number*]

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500. If this parameter is not specified, all the tests are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the configuration information of a test. The configuration information varies with packet types.

Examples

The following example displays the configuration information of ip rns 1.

```
Hostname> enable
Hostname# show ip rns configuration 1
Entry number: 1
Tag: Hostname555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 10000
Threshold (milliseconds): 5000
```

```
Recurring (Starting Everyday): FALSE
Life (seconds): 3500
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 2.2.2.3/0.0.0.0
Request size (ARR data portion): 36
```

Table 1-4 Output Fields of the show ip rns configuration Command

Field	Description
Entry number	Track operation index
Tag	Instance tag
Type of operation to perform	Test type
Operation timeout (milliseconds)	Timeout duration
Operation frequency (milliseconds)	Test repeat interval
Threshold (milliseconds)	Threshold
Recurring (Starting Everyday)	Whether to start repeatedly
Life (seconds)	Time to live
Next Scheduled Start Time	Start time of the next test scheduling
Target address/Source address	Destination/source address
Request size (ARR data portion)	Size of the request packet data

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define
```

Platform Description

N/A

Related Commands

N/A

1.17 show ip rns collection-statistics

Function

Run the **show ip rns collection-statistics** command to display the detailed statistics of a test.

Syntax

show ip rns collection-statistics [*operation-number*]

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500. If this parameter is not specified, all the RNS operation objects are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the result statistics of a test.

Examples

The following example displays the result statistics of all the tests (the ICMP echo test type is taken as an example).

```
Hostname> enable
Hostname# show ip rns collection-statistics 1
Entry number: 1
Start Time Index: *2014-03-20 19:53:51
Last receive time Index: *2020-11-08 06:13:42
Number of successful operations: 919
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 2
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 2
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
Last packet sent sequence: 5

RTT Values:
RTTAvg: 18      RTTMin: 16      RTTMax: 37
NumOfRTT: 919    RTTSum: 16654      RTTSum2: 302786
jitter of operations: 0.000000
Lost packet ratio :0.0000%
```

Table 1-5 Output Fields of the show ip rns collection-statistics Command

Field	Description
Entry number	Track operation index
Start Time Index	Actual test start time (scheduling start time)
Number of successful operations:	Number of successful tests

Field	Description
Number of operations over threshold:	Number of operations over the configured threshold
Number of failed operations due to a Disconnect:	Number of disconnections
Number of failed operations due to a Timeout:	Number of failed operations due to timeout
Number of failed operations due to a Busy:	Number of failed operations because the peer is busy after a packet is sent to the test destination address
Number of failed operations due to a No Connection:	Number of failed operations due to a connection failure
Number of failed operations due to an Internal Error:	Number of failed operations due to an internal error
Number of failed operations due to a Sequence Error:	Number of failed operations due to a sequence error
Number of failed operations due to a Verify Error:	Number of failed operations due to a verification error
RTT Values	Round trip time (RTT) value
RTTAvg:	RTT average of the test
RTTMin:	RTT minimum value of the test
RTTMax:	RTT maximum value of the test
NumOfRTT:	Number of times of counting RTT
RTTSum:	RTT sum of the test
RTTSum2:	RTT square sum of the test
jitter of operations:	Jitter value during the test
Lost packet ratio	Packet loss rate, with four decimal places reserved

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define
```

Platform Description

N/A

Related Commands

N/A

1.18 show ip rns operational-state

Function

Run the **show ip rns operational-state** command to display the current status of a test.

Syntax

show ip rns operational-state [*operation-number*]

Parameter Description

operation-number: Track operation number. The value range is from 1 to 500. If this parameter is not specified, all the tests are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the current status of a test.

Examples

The following example displays the current status information of all the tests.

```
Hostname> enable
Hostname# show ip rns operational-state
Entry number: 1
Modification time: *2014-01-10 10:26:14
Current seconds left in Life: Forever
Operational state of entry: Active
Number of Octets Used by this Entry: 2272
Number of operations attempted: 232
Number of operations skipped: 0
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 4
Latest operation start time: 2014-01-10 10:26:55
Latest operation return code: OK
```

Table 1-6 Output Fields of the show ip rns operational-state Command

Field	Description
Entry number	Track operation index
Modification time	Re-counting time of test results (the results are re-counted after one scheduling starts)
Number of Octets Used by this Entry	Total number of packet bytes sent by the instance
Number of operations attempted	Total number of operations attempted
Number of operations skipped	Total number of operations skipped
Current seconds left in Life	Remaining life of the test
Operational state of entry	Current status (Active or Disactive) of the test
Connection loss occurred	Whether disconnection occurred during the test
Timeout occurred	Whether timeout occurred
Over thresholds occurred	Whether the test result exceeds the threshold
Latest RTT (milliseconds)	RTT of the latest test
Latest operation start time	Latest operation start time
Latest operation return code	Latest operation return code

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define
```

Platform Description

N/A

1.19 show ip rns reaction-configuration

Function

Run the **show ip rns reaction-configuration** command to display the proactive threshold monitoring information of a test.

Syntax

show ip rns reaction-configuration [*operation-number*]

Parameter Description

operation-number: Number of an IP RNS operation object. The value range is from 1 to 500. If this parameter is not specified, all the RNS operation objects are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the proactive threshold monitoring information of a test.

Examples

The following example displays the proactive threshold monitoring information of all the tests.

```
Hostname> enable
Hostname# show ip rns reaction-configuration
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger
Entry number: 2
Reaction: timeout
Threshold Type: Never
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger
```

Table 1-7 Output Fields of the show ip rns reaction-configuration Command

Field	Description
Entry number	Track operation index
Reaction	Threshold monitoring object, such as RTT or timeout
Threshold Type	Threshold trigger action type
Rising (milliseconds)	Upper threshold
Falling (milliseconds)	Lower threshold
Threshold Count	x value when threshold-type is xofy or the average number of times when threshold-type is average
Threshold Count2	y value when threshold-type is xofy or the number of consecutive times when threshold-type is consecutive
Action Type	Action type

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define.
```

Platform Description

N/A

Related Commands

N/A

1.20 show ip rns reaction-trigger

Function

Run the **show ip rns reaction-trigger** command to display the test trigger information of a test.

Syntax

show ip rns reaction-trigger [*operation-number*]

Parameter Description

operation-number: Number of an IP RNS operation object. The value range is from 1 to 500. If this parameter is not specified, all the RNS operation objects are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the test trigger information of a test.

Examples

The following example displays the test trigger information of all the tests.

```
Hostname> enable
Hostname# show ip rns reaction-trigger
Entry number: 1
Target rns index: 2
Status of Entry: active
Operational State: pending
```

Table 1-8 Output Fields of the show ip rns reaction-trigger Command

Field	Description
Entry number	Track operation index

Field	Description
Target rns index	Triggered track index value
Status of Entry	rns_entry status
Operational State	Current trigger status

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define
```

Platform Description

N/A

Related Commands

N/A

1.21 show ip rns statistics

Function

Run the **show ip rns statistics** command to display the brief statistics of a track object.

Syntax

show ip rns statistics [*operation-number*]

Parameter Description

operation-number: Number of an IP RNS operation object. The value range is from 1 to 500. If this parameter is not specified, all the RNS operation objects are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the brief statistics of a track object. The statistics vary with packet types.

Examples

The following example displays the brief statistics of ip rns 1.

```
Hostname> enable
Hostname# show ip rns statistics 1
Entry number: 1
Operation time to live: forever
```

```
Latest RTT: 1
Latest operation start time: 2020-07-31 14:59:07
Latest operation return code: NoConnection/Busy/Timeout
Number of successes: 16
Number of failures: 49
Jitter of rtt time: 2
```

Table 1-9 Output Fields of the show ip rns statistics Command

Field	Description
Entry number	RNS index ID
Operation time to live	Remaining life of the current test
Latest RTT	RTT of the latest test
Latest operation start time	Latest operation start time
Latest operation return code	Latest operation return code (such as ok, timeout, and noconnection)
Number of successes	Number of successful tests
Number of failures	Number of failed tests

Notifications

When the IP track instance is not configured, the following notification will be displayed:

```
rns operate has not define
```

Platform Description

N/A

Related Commands

N/A

1.22 show track

Function

Run the **show track** command to display the statistics of a track object.

Syntax

show track [*object-number*]

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700. If this parameter is not specified, all the track objects are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

Run this command to display the statistics of a track object.

Examples

The following example displays the statistics of all the track objects.

```
Hostname> enable
Hostname# show track
Track 1
  Reliable Network Service 1
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 2
  Interface GigabitEthernet 0/1
  The state is Down
    3 change, current state last: 300 secs
  Delay up 60 secs, down 60 secs
Track 4
  rns-list 1-2 and
  The state is Down
    3 change,current state last:5 secs
  Delay up 0 secs,down 0 secs
```

Table 1-10 Output Fields of the show track Command

Field	Description
Track x	Number of the track object
Reliable Network Service x	Track RNS object
The state is x	Track object state
x change	Number of state change times of the track object
current state last: x secs	Duration of the current track object state
Delay up x secs, down x secs	Delay attribute of the track object
Interface x x	Track interface information
The state is x, delayed y (c secs remaining)	Indicates that the current track object state is x and changes to y after c seconds.

Field	Description
List boolean and	Indicates that the result of the track object is accessed from the AND operation result of all the members.
Object x	Indicates that the meeting condition of member x is its up state.
Object x not	Indicates that the meeting condition of member x is its down state.

Notifications

When the specified track object for display is not configured, the following notification will be displayed:

```
Illegal Value: the track object does not exist.
```

Platform Description

N/A

Related Commands

N/A

1.23 tag

Function

Run the **tag** command to configure a tag for an IP test.

Run the **no** form of this command to remove this configuration.

No test tag is configured by default.

Syntax

tag *tag-name*

no tag

Parameter Description

tag-name: Test tag. The value is a string consisting of a maximum of 79 characters.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

This command specifies a tag for a test, which is often used to indicate the function of the test. When the tag character length exceeds 79, the excess part is automatically truncated.

Examples

The following example configures test instance 1 of ICMP echo type, and sets the test destination IP address of this instance to 10.1.1.1 and tag to telecom_gateway.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# tag telecom_gateway
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 tcp-connect

Function

Run the **tcp-connect** command to configure a TCP test.

No test of TCP type is configured by default.

Syntax

tcp-connect { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } *port-number* [**source-ipaddr** *ipv4-address*] [[**af-direct**] **out-interface** *interface-type interface-number* **next-hop** *ipv4-address*]

Parameter Description

destination-ipv4-address: Destination IPv4 address.

destination-hostname: Destination host name. The maximum length is 127 characters, and the excess part is truncated automatically.

name-server *ipv4-address*: Indicates the IPv4 address of the DNS server. By default, the DNS server configured by running the **ip name-server** command on the device is used for resolution.

port-number: TCP port to be tested. The value range is from 1 to 65535.

source-ipaddr *ipv4-address*: Indicates the source IPv4 address.

af-direct: Indicates that packets are received and sent without passing through the protocol stack in the test.

out-interface *interface-type interface-number*: Specifies the outbound interface type and number for test packets.

next-hop *ipv4-address*: Indicates the next hop IPv4 address when the outbound interface is specified.

Command Modes

IP RNS configuration mode

Default Level

1

Usage Guidelines

After a TCP test is started, the system sets up a TCP connection to test whether the device is connected to the target host. After a TCP IP test is created, the system enters the IP RNS TCP mode.

The TCP test is used to test the performance of establishing a connection with a TCP server. When there is no corresponding TCP server at the peer end, you can start the RNS server on the peer device to complete the test.

Examples

The following example configures test instance 1 of TCP type, and sets the test destination address to www.123.com, DNS server address to 1.1.1.1, and the test TCP port to 999.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config)# tcp-connect www.123.com name-server 1.1.1.1 999
```

Notifications

When you configure a test of TCP type, if the memory allocation fails, the configuration fails and the following notification will be displayed:

```
rns object tcp create fail
```

When you configure a TCP test, if the destination host name exceeds 63 characters, the configuration fails and the following notification will be displayed:

```
rns domain name too long
```

When you configure an incorrect tcp-connect destination host name, the configuration fails and the following notification will be displayed:

```
dns domain name to ip faild
```

Common Errors

- The configured tcp-connect destination host name is incorrect.

Platform Description

N/A

Related Commands

N/A

1.25 threshold

Function

Run the **threshold** command to configure the upper threshold of a test.

Run the **no** form of this command to restore the default configuration.

The default upper threshold of test is **5** seconds.

Syntax

threshold *interval*

no threshold

Parameter Description

interval: Upper threshold of a test, in milliseconds. The value range is from 0 to 60000.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

The configured threshold must be less than or equal to timeout. For the configuration relationship between timeout, frequency, and threshold, see the usage guidelines for frequency.

Examples

The following example configures test instance 1 of ICMP echo type, and specifies the test destination address as 10.1.1.1. The upper threshold of test is set to 8000 milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# threshold 8000
```

Notifications

When the configured threshold is greater than timeout, the following notification will be displayed:

```
Illegal Value: Cannot set Threshold to be greater than Timeout.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 timeout

Function

Run the **timeout** command to configure the timeout interval of a test.

Run the **no** form of this command to restore the default configuration.

The default timeout interval of a test is **5** seconds.

Syntax

timeout *interval*

no timeout

Parameter Description

interval: Timeout interval of the test, in milliseconds. The value range is from 10 to 604800000.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

The configured timeout interval must be greater than or equal to the configured threshold. For the configuration relationship between timeout, frequency, and threshold, see the usage guidelines for frequency.

Examples

The following example configures test instance 1 of ICMP echo type, specifies the test destination IP address as 10.1.1.1, and sets the timeout interval to 10000 milliseconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# timeout 10000
```

Notifications

When you configure a timeout interval greater than the frequency value, the configuration fails and the following notification will be displayed:

```
Illegal Value: Cannot set Timeout to be greater than Frequency.
```

When you configure a timeout interval smaller than the threshold value, the configuration fails and the following notification will be displayed:

```
Illegal Value: Cannot set Timeout to be less than Threshold.
```

Common Errors

- The configured timeout interval is greater than the frequency value.
- The configured timeout interval is smaller than the threshold value.

Platform Description

N/A

Related Commands

N/A

1.27 tos

Function

Run the **tos** command to configure the type of service (TOS) field in the IPv4 packet of a test.

Run the **no** form of this command to remove this configuration.

The default TOS value for IPv4 packet of the test is **0**.

Syntax

tos *tos-value*

no tos

Parameter Description

tos-value: TOS field in the IPv4 packet of a test. The value range is from 0 to 255.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

TOS is an 8-bit field in the IPv4 packet header. You can set the TOS field to control the priority of the test packet. For different TOS fields, the processing priorities are different on the intermediate devices.

Examples

The following example configures an ICMP echo test, specifies the destination address of the test as 10.1.1.1, and sets the TOS value in IPv4 test packet header to 128.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# tos 128
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 track interface line-protocol

Function

Run the **track interface line-protocol** command to configure a track object, which is used to track the link status of an interface.

Run the **no** form of this command to remove this configuration.

The function of clearing all the tests is not configured by default.

Syntax

track *object-number* **interface** *interface-type interface-number* **line-protocol**

no track *object-number*

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700.

I*nterface-type interface-number*: Type and number of the interface.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Run this command to configure a track object for tracking the link status of an interface. When the link status of the interface is up, the status of the corresponding track object is also up.

Examples

The following example configures track object 3, which is used to track the link status of the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 3 interface GigabitEthernet 0/1 line-protocol
```

Notifications

When a track object is configured, if the resource on the device is insufficient, the following notification will be displayed:

```
Failed to create track obj, no resource.
```

When you run the **no track** command to delete a specified track object, if the track object is not configured on the device, the following notification will be displayed:

```
the track object does not exist.
```

Common Errors

- The track object for tracking the link status of an interface is configured, but the corresponding interface is not configured.

Platform Description

N/A

Related Commands

N/A

1.29 track list

Function

Run the **track list** command to configure a track object for tracking the status of a track list.

Run the **no** form of this command to remove this configuration.

No status is configured for a track list by default.

Syntax

track *object-number* **list boolean** { **and** | **or** }

no track *object-number*

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Run this command to configure a track object for tracking the status of a track list. The result can be the AND or OR operation result of all member status.

track *object-number* **list boolean and**: Configures a track object to track the status of a track list. The result is the AND operation result of all member status.

track *object-number* **list boolean or**: Configures a track object to track the status of a track list. The result is the OR operation result of all member status.

Examples

The following example configures track object 4, which is used to track the status of a track list. The result is the AND operation result of all member status.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 4 list boolean and
```

Related Commands

Run the **show track** command to display the statistics of a track object.

Notifications

When a track object is configured, if the resource on the device is insufficient, the following notification will be displayed:

```
Failed to create track obj, no resource.
```

When you run the **no track** command to delete a specified track object, if the track object is not configured on the device, the following notification will be displayed:

```
the track object does not exist.
```

Common Errors

- The track object for tracking the status of a track list is configured, but no member of the track list is configured.

Platform Description

N/A

Related Commands

N/A

1.30 track rns

Function

Run the **track rns** command to configure a track object, which is used to track the test result of a track instance.

Run the **no** form of this command to remove this configuration.

No track test result is configured by default.

Syntax

track *object-number* **rns** *entry-number*

no track *object-number*

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700.

entry-number: Track operation number. The value range is from 1 to 500.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Run this command to configure a track object for tracking the test result of a track instance. When the track instance test succeeds, the corresponding track object is in up status.

Examples

The following example configures track object 5 for tracking track instance 7.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 5 rns 7
```

Notifications

When a track object is configured, if the resource on the device is insufficient, the following notification will be displayed:

```
Failed to create track obj, no resource.
```

When you run the **no track** command to delete a specified track object, if the track object is not configured on the device, the following notification will be displayed:

```
the track object does not exist.
```

Common Errors

- The track object for tracking an RNS test is configured, but the corresponding track instance is not configured.

Platform Description

N/A

Related Commands

N/A

1.31 track rns-list

Function

Run the **track rns-list** command to configure a track object, which is used to track the test result of an rns-list instance.

Run the **no** form of this command to remove this configuration.

No object of track test result is configured by default.

Syntax

track *object-number* **rns-list** *men-list* { **and** | **or** }

no track *object-number*

Parameter Description

object-number: Number of a track object. The value range is from 1 to 700.

men-list: Tracked RNS list. Here, men-list can be an RNS test instance or a series of RNS test instances. If men-list is a series of RNS IDs, the format is as follows: Minimum RNS ID-Maximum RNS ID, for example, 10-20. The value range of RNS ID is from 1 to 500.

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

Run this command to configure a track object for tracking the status of an RNS list. The result can be the AND or OR operation result of all member status.

track object-number rns-list men-list and: Configures a track object to track the status of a track list. The result is the AND operation result of all member status.

track *object-number* **rns-list** *men-list* **or**: Configures a track object to track the status of an RNS list. The result is the OR operation result of all member status.

Examples

The following example configures track object 5 for tracking track instances 1, 2-5, and 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# track 5 rns-list 1,2-5,8 and
```

Notifications

When a track object is configured, if the resource on the device is insufficient, the following notification will be displayed:

```
Failed to create track obj, no resource.
```

When you run the **no track** command to delete a specified track object, if the track object is not configured on the device, the following notification will be displayed:

```
the track object does not exist.
```

Common Errors

- The track object for tracking rns-list is configured, but the corresponding track instance is not configured.

Platform Description

N/A

Related Commands

N/A

1.32 udp-echo

Function

Run the **udp-echo** command to configure a test object of UDP echo type.

No test object of UDP echo type is configured by default.

Syntax

udp-echo { **oob** *destination-ipv4-address port-number* [**via** *interface-type interface-number* **next-hop** *next-hop-ip*] | *destination-ipv4-address port-number* [**out-interface** *interface-type interface-number* **next-hop** *next-hop-ip*] }

udp-echo *destination-ipv4-address port-number* [**out-interface** *interface-type interface-number* **next-hop** *next-hop-ip*]

Parameter Description

oob: Indicates the test on the MGMT port.

destination-ipv4-address: Destination IP address.

port-number: Destination port.

out-interface *interface-type interface-number*: Specifies the outbound interface (not the MGMT port) for test packets.

next-hop *next-hop-ip*: Indicates the next hop IP address.

via *interface-type interface-number*: Specifies the outbound interface (MGMT port) for the test packets.

Command Modes

IP RNS configuration mode

Default Level

1

Usage Guidelines

You must enable the RNS server at the peer end of the test to implement a UDP echo test.

The value of *port-number* must be consistent with the port number configured for the RNS server.

Examples

The following example configures test instance 1 of UDP echo type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# udp-echo 10.10.10.1 1025
Hostname(config-ip-rns-udp-echo)#
```

Notifications

When you configure a test of UDP echo type, if the memory allocation fails, the configuration fails and the following notification will be displayed:

```
rns object entry %d create fail
```

Common Errors

- The configured udp-echo destination host name is incorrect.

Platform Description

N/A

Related Commands

N/A

1.33 vrf

Function

Run the **vrf** command to configure the VRF of a test.

Run the **no** form of this command to remove this configuration.

No VRF name is configured for the test by default.

Syntax

vrf *vrf-name*

no vrf

Parameter Description

vrf-name: Virtual routing and forwarding (VRF) name.

Command Modes

IP RNS DNS configuration mode

IP RNS ICMP-Echo configuration mode

IP RNS TCP configuration mode

IP RNS UDP-Echo configuration mode

Default Level

1

Usage Guidelines

This command specifies the VRF of the test packet.

Examples

The following example configures test instance 1 of ICMP echo type, and specifies the test destination address as 10.1.1.1 and the VRF of the test as VPN1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip rns 1
Hostname(config-ip-rns)# icmp-echo 10.1.1.1
Hostname(config-ip-rns-icmp-echo)# vrf VPN1
```

Notifications

When the specified VRF name is invalid, the configuration fails and the following notification will be displayed:

```
no vrf named.
```

Common Errors

- The specified VRF name is invalid.

Platform Description

N/A

Related Commands

N/A

1 IP Event Dampening Commands

Command	Function
dampening	Enable the function of IP Event Dampening.
show dampening interface	Display the statistics about interfaces with IP Event Dampening.
show interfaces dampening	Display IP Event Dampening configurations on an interface.

1.1 dampening

Function

Run the **dampening** command to enable the function of IP Event Dampening.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of IP Event Dampening is disabled for a routing interface by default.

Syntax

dampening [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]

no dampening

default dampening

Parameter Description

half-life-period: Half-life period in seconds. The value range is from 1 to 30. The default value is **5**.

reuse-threshold: Reuse threshold. The value range is from 1 to 20000. The default value is **1000**.

suppress-threshold: Suppress threshold. The value range is from 1 to 20000. The default value is **2000**.

max-suppress: Maximum suppress time. The value range is 1 to 255. The default value is four times that of *half-life-period*.

restart *restart-penalty*: Specifies the initial penalty. The value range is from 1 to 20000. The default value is **2000**.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Configuring the function of IP Event Dampening affects the functions of associated modules (direct routes, host routes, static routes, dynamic routes, and Virtual Router Redundancy Protocol (VRRP)).

When an interface is suppressed based on the configured criteria of the command, the associated modules determine the interface as Down and thus delete corresponding routes. This interface does not receive and send any data.

When the **dampening** command is reconfigured on an interface configured with this command, the dampening information on the interface is cleared, but the flap count is retained, unless you run the **clear counters** command to clear the interface statistics.

Examples

The following example enables IP Event Dampening on interface GigabitEthernet0/1, and sets the half-time period to 30s, the reuse threshold to 1500, the suppress threshold to 10,000, and the maximum suppress time to 100s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

Notifications

When the configured maximum suppress time (*max-suppress*) is so small that the maximum penalty is smaller than the suppress threshold, the interface is never suppressed. When such a configuration error occurs, the following notification will be displayed:

```
% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time
```

When the **damening** command is configured and the available system memory is insufficient to save the configuration, the following notification will be displayed:

```
% No memory, configure dampening fail!
```

Common Errors

- The configured maximum suppress time (*max-suppress*) is too small.
- IP Event Dampening is configured on an non-L3 interface.

Platform Description

This command is supported on only L3 devices.

When a routed interface is converted into a switching interface, the **dampening** command configured on the interface is deleted.

IP Event Dampening cannot be configured on **virtual templates**.

Related Commands

- **show dampening interface**
- **show interfaces dampening**

1.2 show dampening interface

Function

Run the **show dampening interface** command to display the statistics about interfaces with IP Event Dampening.

Syntax

show dampening interface

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display statistics about interfaces with IP Event Dampening.

Examples

The following example displays statistics about interfaces with IP Event Dampening.

```
Hostname> enable
Hostname# show dampening interface
1 interfaces are configured with dampening.
No interface is being suppressed.
```

Table 1-1 Output Fields of the show dampening interface Command

Field	Description
interfaces are configured with dampening	Number of interface configured with Event Dampening
interface is being suppressed	Number of the suppressed interfaces

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show interfaces dampening**

1.3 show interfaces dampening

Function

Run the **show interfaces dampening** command to display IP Event Dampening configurations on an interface.

Syntax

show interfaces [*interface-type interface-number*] **dampening**

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, information about all interfaces is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays IP Event Dampening configurations.

```
Hostname> enable
Hostname# show interfaces dampening
GigabitEthernet 0/1
  Flaps Penalty Supp    ReuseTm HalfL   ReuseV  SuppV   MaxSTm  MaxP    Restart
  0     0       FALSE   0       30      1500    10000   100     15119   0
```

Table 1-2 Output Fields of the show interfaces dampening Command

Field	Description
Flaps	Number of flaps of an interface
Penalty	Current penalty value
Supp	Whether an interface is suppressed
ReuseTm	Remaining time for an interface to be reused in seconds
HalfL	Half-life period
ReuseV	Reuse threshold
SuppV	Suppress threshold
MaxSTm	Maximum suppress time
MaxP	Maximum penalty
Restart	Initial penalty

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show dampening interface**

1 HAM Commands

Command	Function
ham single-process-ha auto-restart enable	Enable the high availability (HA) service of one frequently restarting process.

1.1 ham single-process-ha auto-restart enable

Function

Run the **ham single-process-ha auto-restart enable** command to enable the high availability (HA) service of one frequently restarting process.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The HA service of one frequently restarting process is enabled by default.

Syntax

ham single-process-ha auto-restart enable

no ham single-process-ha auto-restart enable

default ham single-process-ha auto-restart enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Before a patch upgrade, you can disable the HA service of one frequently restarting process. After a patch upgrade, you can enable the HA service of one frequently restarting process when confirming that no process restarts frequently.

Caution

If you disable the HA service of one frequently restarting process by running a command, services may not be automatically restored to normal because some processes frequently restart due to no automatic restarting of the device. As a result, failure time prolongs. Therefore, you are advised to enable the configuration in scenarios other than patch upgrades.

Examples

The following example disables the HA service of one frequently restarting process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ham single-process-ha auto-restart enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Network Management and Monitoring Commands

1 Network Connectivity Test Commands

Command	Function
clear rping table	Clear the remote Ping (Rping) table entries.
ping ip	Check whether the specified IPv4 address is reachable and output the related information.
ping ipv6	Check whether the specified IPv6 address is reachable and output the related information.
show rping detail	Display the details about Rping table entries.
traceroute ip	Display the routing devices through which IPv4 packets are sent from the source address to the destination address.
traceroute ipv6	Display the gateways through which IPv6 packets are sent from the source address to the destination address.

1.1 clear rping table

Function

Run the **clear rping table** command to clear the remote Ping (Rping) table entries.

Syntax

clear rping table { **all** | **ping-object** *owner-index test-index* | **trace-object** *owner-index test-index* }

Parameter Description

all: Deletes all entries of the Rping table.

owner-index: Index of a user.

test-index: Index of a test.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After this command is executed, Rping table entries are deleted based on the specified parameters.

The Rping table stores the results of Ping tests executed by users through Simple Network Management Protocol (SNMP).

Examples

The following example clears all entries of the Rping table.

```
Hostname> enable
Hostname# clear rping table all
```

The following example clears the Rping table entry where the user index is **user** and the test index is **Hostname**.

```
Hostname> enable
Hostname# clear rping table user Hostname
```

Notifications

When no specified entry exists on the device, the following notification will be displayed:

Platform Description

N/A

Related Commands

N/A

1.2 ping ip

Function

Run the **ping ip** command to check whether the specified IPv4 address is reachable and output the related information.

By default, five 100-byte packets are sent to the specified IP address within two seconds.

Syntax

ping [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* } [**data** *data* | **detail** | **df-bit** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **validate**] *

ping oob { *hostname* | *ipv4-address* } [**data** *data* | **detail** | **df-bit** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **validate** | **via** *mgmt-name*] *

Parameter Description

vrf *vrf-name*: Specifies a VRF. If this parameter is not specified, the public network instance is used.

hostname: Destination host name.

ipv4-address: Destination IPv4 address.

data *data*: Specifies the padding data of the packet. The format is a string of 1 to 255 characters. By default, **abcd** is padded.

detail: Configures whether to display the detailed information. By default, only the exclamation mark (!) and period (.) are displayed.

df-bit: Configures the DF bit of the IP address. If the DF bit is set to 1, the packet is not segmented. The default value is 0.

interval *interval*: Specifies the interval between the Ping packets, in milliseconds. The value range is from 50 to 300000, and the default value is **100**.

length *length*: Specifies the length of the padding section in the sent packet, in bytes. The value range is from 36 to 18024, and the default value is **100**.

ntimes *times*: Specifies the number of sent packets. The value range is from 1 to 4294967295. The default value is **5**.

out-interface *interface-type interface-number*: Specifies the type and number of the outbound interface used to send the packets.

next-hop *next-hop*: Specifies the IPv4 address of the next hop of the outbound interface used to send the packets.

source *interface-type interface-number*: Specifies the type and number of the source interface of the packets.

source *source-ipv4-address*: Specifies the source IPv4 address or source interface of the packets. A loopback interface, for example, 127.0.0.1, cannot be configured as the source address.

timeout *time*: Specifies the timeout, in seconds. The value range is from 1 to 10, and the default value is **2**.

validate: Configures whether to verify the response packet.

oob: Indicates that an out-of-band channel is used. This parameter is mandatory if the MGMT interface is configured as the source interface.

via *mgmt-name*: Specifies the outbound MGMT interface of packets where the Ping operation is performed.

Command Modes

Privileged EXEC mode

Default Level

0

Usage Guidelines

After this command is executed, the related response information is printed and then the statistical information is output.

To use the domain name function, you must first configure the domain name server (DNS). For details, see "Configuring DNS" in "IP Service Configuration Guide."

Examples

The following example checks whether the IPv4 address 192.168.21.26 is reachable.

```
Hostname> enable
Hostname# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example checks whether the IPv4 address 192.168.21.26 is reachable. The sent packet length is 1500 bytes, the number of sent packets is 10, the timeout is 3 seconds, the packet padding data is ffff, and the source IP address is 192.168.21.99.

```
Hostname> enable
Hostname# ping 192.168.21.26 length 1500 ntimes 10 data ffff source 192.168.21.99
timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/3 ms.
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ping ipv6

Function

Run the **ping ipv6** command to check whether the specified IPv6 address is reachable and output the related information.

By default, five 100-byte packets are sent to the specified IPv6 address within two seconds.

Syntax

ping [**ipv6** | **vrf** *vrf-name*] { *hostname* | *ipv6-address* } [**data** *data* | **detail** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time*] *

ping oob { *hostname* | *ipv6-address* } [**data** *data* | **detail** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time* | **validate** | **via** *mgmt-name*] *

Parameter Description

vrf *vrf-name*: Specifies a VRF. If this parameter is not specified, the public network instance is used.

hostname: Destination host name.

ipv6-address: Destination IPv6 address.

data *data*: Specifies the padding data of the packet. The format is a string of 1 to 255 characters. By default, **abcd** is padded.

detail: Configures whether to display the detailed information. By default, only the exclamation mark (!) and period (.) are displayed.

interval *interval*: Specifies the interval between the Ping packets, in milliseconds. The value range is from 50 to 300000, and the default value is **100**.

length *length*: Specifies the length of the sent packet, in bytes. The value range is from 16 to 18024, and the default value is **100**.

ntimes *times*: Specifies the number of sent packets. The value range is from 1 to 4294967295. The default value is **5**.

out-interface *interface-type interface-number*: Specifies the type and number of the outbound interface used to send the packets.

next-hop *next-hop*: Specifies the IPv6 address of the next hop of the outbound interface used to send the packets.

source *interface-type interface-number*: Specifies the type and number of the source interface of the packets.

source *source-ipv6-address*: Specifies the source IPv6 address or source interface of the packets. A loopback interface, for example, ::1, cannot be configured as the source address.

timeout *time*: Specifies the timeout, in seconds. The value range is from 1 to 10, and the default value is **2**.

oob: Indicates that an out-of-band channel is used. This parameter is mandatory if the MGMT interface is configured as the source interface.

via *mgmt-name*: Specifies the outbound MGMT interface of packets where the Ping operation is performed.

Command Modes

Privileged EXEC mode

Default Level

0

Usage Guidelines

After this command is executed, the related response information is printed. If the data in the response is inconsistent with the data in the request, "Request receive error" is displayed, and then the statistical information is output.

To use the domain name function, you must first configure the domain name server (DNS). For details, see "Configuring DNS" in "IP Service Configuration Guide."

Examples

The following example checks whether the IPv6 address 2001::5 is reachable.

```
Hostname> enable
Hostname# ping ipv6 2001::5
Sending 5, 100-byte ICMP Echoes to 2001::5, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example checks whether the IPv6 address 2001::5 is reachable. The sent packet length is 1500 bytes, the number of sent packets is 10, the timeout is 3 seconds, the packet padding data is ffff, and the source IP address is 2001::9.

```
Hostname> enable
Hostname#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
```

```
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show rping detail

Function

Run the **show rping detail** command to display the details about Rping table entries.

Syntax

show rping detail

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can use this command to view the number of users and the number of tests in the Rping table on a device.

Examples

The following example displays detailed information of Rping table entries.

```
Hostname> enable
Hostname# show rping detail
Total owner number: 2
Total test number: 4
owner: user1
   test name: taget_1        storage type: volatile
```

```
test name: taget_2        storage type: nonVolatile
owner: user2
  test name: taget_1        storage type: permanent
test name: taget_2        storage type: readOnly
```

Table 1-1 Output Fields of the show rping detail Command

Field	Description
Total owner number	Total number of users
Total test number	Total number of tests
owner	Username
test name	Name of a test
storage type	Storage type of a table entry

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 traceroute ip

Function

Run the **traceroute ip** command to display the routing devices through which IPv4 packets are sent from the source address to the destination address.

By default, the timeout is **3** seconds, the number of sent probe packets is **3**, the minimum TTL is **1**, and the maximum TTL is **255**.

Syntax

traceroute [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

traceroute oob { *hostname* | *ipv4-address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **ttl** *minimum maximum* | **via** *mgmt-name*] *

Parameter Description

vrf *vrf-name*: Specifies a VRF. If this parameter is not specified, the public network instance is used.

hostname: Destination host name.

ipv4-address: Destination IPv4 address.

out-interface *interface-type interface-number*: Specifies the type and number of the outbound interface used to send the packets.

next-hop *next-hop*: Specifies the IPv4 address of the next hop of the outbound interface used to send the packets.

probe *probe*: Specifies the number of sent probe packets. The value range is from 1 to 255, and the default value is **3**.

source *interface-type interface-number*: Specifies the type and number of the source interface of the packets.

source *source-ip-address*: Specifies the source IPv4 address or source interface of the packets. A loopback interface, for example, 127.0.0.1, cannot be configured as the source address.

timeout *time*: Specifies the timeout, in seconds. The value range is from 1 to 10, and the default value is **3**.

ttl *minimum maximum*: Specifies the minimum and maximum TTL values. The value range is from 1 to 255. By default, the minimum TTL is **1**, and the maximum TTL is **255**.

oob: Indicates that an out-of-band channel is used. This parameter is mandatory if the MGMT interface is configured as the source interface.

via *mgmt-name*: Specifies the outbound MGMT interface of packets where the Traceroute operation is performed.

Command Modes

Privileged EXEC mode

Default Level

0

Usage Guidelines

You can run this command to check the network connectivity, and accurately determine the location of a network fault when the fault occurs.

To use the domain name function, you must first configure the domain name server (DNS). For details, see "Configuring DNS" in "IP Service Configuration Guide."

Examples

The following example displays the gateways through which IPv4 packets are sent from the source address to the destination address 61.154.22.36.

```
Hostname> enable
Hostname# traceroute 61.154.22.36
< press Ctrl+C to break >
Tracing the route to 61.154.22.36
1     192.168.12.1    0 msec  0 msec  0 msec
2     192.168.9.2     4 msec  4 msec 4 msec
3     192.168.9.1     8 msec  8 msec  4 msec
4     192.168.0.10    4 msec  28 msec  12 msec
5     202.101.143.130    4 msec  16 msec  8 msec
6     202.101.143.154   12 msec  8 msec  24 msec
```

```
7     61.154.22.36    12 msec  8 msec  22 msec
```

The following example displays the gateways through which IPv4 packets are sent from the source address to the destination domain name www.ietf.org.

```
Hostname> enable
Hostname# traceroute www.ietf.org
Translating " www.ietf.org "...[OK]
< press Ctrl+C to break >
Tracing the route to 64.170.98.32
1     192.168.217.1   0 msec  0 msec  0 msec
2     10.10.25.1        0 msec  0 msec  0 msec
3     10.10.24.1        0 msec  0 msec  0 msec
4     10.10.30.1        10 msec 0 msec  0 msec
5     218.5.3.254       0 msec  0 msec  0 msec
6     61.154.8.49       10 msec 0 msec  0 msec
7     202.109.204.210    0 msec  0 msec  0 msec
8     202.97.41.69      20 msec 10 msec 20 msec
9     202.97.34.65      40 msec 40 msec 50 msec
10    202.97.57.222     50 msec 40 msec 40 msec
11    219.141.130.122   40 msec 50 msec 40 msec
12    219.142.11.10     40 msec 50 msec 30 msec
13    211.157.37.14     50 msec 40 msec 50 msec
14    222.35.65.1       40 msec 50 msec 40 msec
15    222.35.65.18      40 msec 40 msec 40 msec
16    222.35.15.109     50 msec 50 msec 50 msec
17    *      *      *
18   64.170.98.32     40 msec 40 msec 40 msec
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 traceroute ipv6

Function

Run the **traceroute ipv6** command to display the gateways through which IPv6 packets are sent from the source address to the destination address.

By default, the timeout is **3** seconds, the number of sent probe packets is **3**, the minimum TTL is **1**, and the maximum TTL is **255**.

Syntax

traceroute [**ipv6** | **vrf** *vrf-name*] { *hostname* | *ipv6-address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

traceroute oob { *hostname* | *ipv6-address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time* | **ttl** *minimum maximum* | **via** *mgmt-name*] *

Parameter Description

vrf *vrf-name*: Specifies a VRF. If this parameter is not specified, the public network instance is used.

hostname: Destination host name.

ipv6-address: Destination IPv6 address.

out-interface *interface-type interface-number*: Specifies the type and number of the outbound interface used to send the packets.

next-hop *next-hop*: Specifies the IPv6 address of the next hop of the outbound interface used to send the packets.

probe *probe*: Specifies the number of sent probe packets. The value range is from 1 to 255, and the default value is **3**.

source *interface-type interface-number*: Specifies the type and number of the source interface of the packets.

source *source-ipv6-address*: Specifies the source IPv6 address or source interface of the packets. A loopback interface, for example, ::1, cannot be configured as the source address.

timeout *time*: Specifies the timeout, in seconds. The value range is from 1 to 10, and the default value is **3**.

ttl *minimum maximum*: Specifies the minimum and maximum TTL values. The value range is from 1 to 255. By default, the minimum TTL is **1**, and the maximum TTL is **255**.

oob: Indicates that an out-of-band channel is used. This parameter is mandatory if the MGMT interface is configured as the source interface.

via *mgmt-name*: Specifies the outbound MGMT interface of packets where the Traceroute operation is performed.

Command Modes

Privileged EXEC mode

Default Level

0

Usage Guidelines

You can run this command to check the network connectivity, and accurately determine the location of a network fault when the fault occurs.

To use the domain name function, you must first configure the domain name server (DNS). For details, see "Configuring DNS" in "IP Service Configuration Guide."

Examples

The following example displays the gateways through which IPv6 packets are sent from the source address to the destination address 3004::1.

```
Hostname> enable
Hostname# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     3004::1        4 msec  28 msec  12 msec
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Tech-Support Commands

Command	Function
debug support	Enter the debug support mode.
execute diagnose-cmd	Run the diagnose command.
tech-support package	Collect the detailed fault information of the device.
@@@@f	Collect the detailed fault information of the device by using the hotkey.

1.1 debug support

Function

Run the **debug support** command to enter the debug support mode.

Syntax

debug support

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command is used to enter the debug support mode. You can run the Tech-Support commands only in debug support mode.

Examples

The following example enters the debug support mode.

```
Hostname> enable
Hostname# debug support
%Warning: Enter debug support mode, all commands in this mode are used to diagnose system hardware and software.
        Misuse of these commands will affect system performance. Therefore, use these commands under the guidance of Ruijie Networks engineers.
Hostname(support)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 execute diagnose-cmd

Function

Run the **execute diagnose-cmd** command to run the diagnose command.

Syntax

execute diagnose-cmd { [**device** *device-id*] [**slot all** | **slot** *slot-id* }] [**chip** *chip-id*] *shell-command* | **help** }

Parameter Description

device *device-id*: Indicates the ID of a device.

slot all: Indicates that the diagnose command is executed on all cards.

slot *slot-id*: Indicates that the diagnose command is executed on the specified board. **m*** indicates the management engine, **fe*** indicates the switch fabric module, and 1~* indicates the service interface board. * indicates a positive integer number.

chip *chip-id*: ID of a chip. The value range is from 0 to 7.

shell-command: String of the shell command to be executed. For details about the command string, see Table 1-1.

help: Displays a list of executable *shell commands.*

Command Modes

Debug support mode

Default Level

15

Usage Guidelines

Table 1-1 Description of shell Command Strings

Command	Description
at	**at** diagnose command. Whether the **at** diagnose command is supported depends on the actual product.
copy	Copies files.
delete	Deletes files.
df	Displays the disk space usage.
dir	Displays the file list of the directory.
dmesg	Displays the core logs.
du	Displays the space usage of the file system.
echo	Saves data to a target file.
fdisk	Displays the partitioning information of a device.

Command	Description
hexdump	Displays the file information in hexadecimal format.
kill	Sends a signal to a specified process.
md5sum	Calculates and checks the MD5 message digest.
mkdir	Creates a directory.
more	Displays the file information.
mount	Displays the mounted file system.
process	Stops, starts, or restarts a process or a kernel module with the startup script.
ps	Displays information of the current process.
redis-cli	Database diagnose command
rmdir	Deletes an empty directory.
sdk	sdk diagnose command ● If the chip field is entered, only the sdk command can be executed. ● If the chip field is not entered, the sdk command is executed and the chip value is 0 by default.
sh	Runs the module diagnose shell command.
stat	Displays the file or file system status.
sync	Updates the file system cache.
tftp-tipc	Transfers files through TFTP TIPC between different devices or cards.
tipc-config	Displays the TIPC neighbor node information.
top	Displays the process information.
touch	Creates an empty file or changes the timestamp of a file.
zlog	Displays the zlog file information. For details about the zlog command format, see Table 1-2.

Table 1-2 zlog Command Format

Command	Description
module-name process-name { **debug** | **error** | **fatal** | **info** | **notice** | **warn** }	Displays different levels of log files of a process on a module. Parameter description: ● *module-name*: Name of a module ● *process-name*: Name of a process ● **debug**: Debug level ● **error**: Error level ● **fatal**: Fatal level ● **info**: Information level ● **notice**: Notification level ● **warn**: Warning level

Examples

The following example displays the device configuration file.

```
Hostname> enable
Hostname# debug support
Hostname(support)#execute diagnose-cmd more /data/config.text
```

Notifications

When the diagnosed slot ID is not configured, the following notification will be displayed:

```
% Execute command fail, because tipc connect fail!
```

When the diagnosed chip is not configured, the following notification will be displayed:

```
RG_AT command execute begin.
Chip id is invalid in this device, Please check the chip id!
RG_AT command execute end.
```

When the diagnosed device is not configured, the following notification will be displayed:

```
% Execute command fail, because tipc connect fail!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **debug support**

1.3 tech-support package

Function

Run the **tech-support package** command to collect the detailed fault information of the device.

Syntax

tech-support package [*component-name* | **basic**]

Parameter Description

component-name: Specified component whose fault information is to be collected.

basic: Collects the basic fault information of the device.

Command Modes

Debug support mode

Default Level

14

Usage Guidelines

- This command is used to collect the detailed real-time fault information of each service component and dump file registered with the TECH-SUPPORT framework, and save them in a fault information compressed package. The compressed package name indicates the VSD for which the fault information is collected.
- The fault information compressed package is stored in the descending order of USB flash drive, **Flash:/**, and **Tmp:/**. Before running this command, you are advised to insert the USB flash drive to avoid information loss. You can use the TFTP function to transfer the compressed packages of the final fault information to a PC.
- To prevent excessive consumption of space on the storage media after the fault information is collected for multiple times, a maximum of three compressed packages of fault information can be stored on the same storage medium.
- The compressed packages of fault information are stored as follows:
  - USB flash drive

    If a USB flash drive is inserted into the device, the compressed packages are stored in the root directory of the USB flash drive. You can run the **dir usb0:** command to view these compressed packages.
  - Flash directory

    If no USB flash drive is inserted into the device, the compressed packages are preferentially stored in the Flash directory. You can run the **dir flash:** command to view these compressed packages.
  - **Tmp** directory (memory)

    If no USB flash drive is inserted into the device and the Flash has insufficient space, the compressed packages are stored in the **Tmp** directory. You can run the **dir tmp:** command to view these compressed packages.

Examples

The following example collects the detailed fault information of the device.

```
Hostname> enable
```

```
Hostname# debug support
Hostname(support)# tech-support package
```

Notifications

- When the fault information of VSD 0 is successfully collected and packaged, the following notifications will be displayed, depending on the type of the storage medium:

  If the fault information compressed package is stored on the USB flash drive of VSD 0, run the **dir usb0:** command to view the package.

  ```
  Tech-support package success, the package file is
  /mnt/usb0/tech_vsd0_20140825164828.tar.gz.
  ```

  If the fault information compressed package is stored in the Flash directory on VSD 0, run the **dir flash:** command to view the package.

  ```
  Tech-support package success, the package file is
  /data/tech_vsd0_20140825164828.tar.gz.
  ```

  If the fault information compressed package is stored in the **Tmp** directory on VSD 0, run the **dir tmp:** command to view the package.

  ```
  Tech-support package success, the package file is
  /tmp/tech_vsd0_20140825164828.tar.gz.
  ```

- When the fault information of VSD 1 is successfully collected and packaged, the following notifications will be displayed, depending on the type of the storage medium:

  If the fault information compressed package is stored on the USB flash drive of VSD 1, run the **dir usb0:** command to view the package.

  ```
  Tech-support package success, the package file is
  /mnt/usb0/tech_vsd1_20140825164829.tar.gz.
  ```

  If the fault information compressed package is stored in the Flash directory on VSD 1, run the **dir flash:** command to view the package.

  ```
  Tech-support package success, the package file
  is/data/var/run/vsd/1/tech_vsd1_20140825175652.tar.gz.
  ```

  If the fault information compressed package is stored in the **Tmp** directory on VSD 1, run the **dir tmp:** command to view the package.

  ```
  Tech-support package success, the package file is
  /tmp/vsd/1/tech_vsd1_20140825164828.tar.gz.
  ```

- When the fault information is successfully collected but fails to be packaged, the following notification will be displayed:

  ```
  Tech-support package failed, the dump file is in dir: /data/tech_vsd0.
  ```

Common Errors

If the storage medium has insufficient space, information fails to be collected in the Tech-Support operation.

Platform Description

N/A

Related Commands

- **debug support**

1.4 @@@@f

Function

Run the @@@@**f** command to collect the detailed fault information of the device by using the hotkey.

Syntax

@@@@**f**

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

N/A

Usage Guidelines

This command is used to collect the detailed fault information of the device by using the hotkey. The @@@@**f** hotkey operation is often performed when the console crashes. The fault information is packaged in a way similar to the **tech-support package** command. The fault information is stored in the descending order of USB flash drive, **Flash:/**, and **Tmp:/**. Before running this command, you are advised to insert the USB flash drive to avoid information loss.

This command takes effect only when the device is connected to the console port, and is invalid for remote connections, for example, Telnet or SSH connection.

Examples

The following example collects the detailed fault information of a management board by using the hotkey.

You only need to press "@@@@f" on the console to trigger the information collection.

Notifications

When the fault information is successfully collected but fails to be packaged, the following notification will be displayed:

```
Tech-support package failed, the dump file is in directory: /data/tech_vsd0.
```

Common Errors

If the storage medium has insufficient space, information fails to be collected in the Tech-Support operation.

Platform Description

N/A

Related Commands

N/A

1 SPAN Commands

Command	Function
default monitor session	Delete all switch port analyzer (SPAN) sessions.
destination ip address	Configure the destination IP address when the encapsulation type is GRE.
ip dscp	Configure the DSCP value for an encapsulated IP packet.
ip ttl	Configure the TTL value for an encapsulated IP packet.
mac-loopback	Enable the MAC loopback function of an interface.
monitor session destination interface	Configure a destination port for a local SPAN session.
monitor session destination remote vlan interface	Configure an output port on an RSPAN source device or a destination port on an RSPAN destination device for an RSPAN session.
monitor session erpsan-source	Create an ERSPAN session.
monitor session filter vlan	Exclude one or more VLANs as the data source of SPAN.
monitor session remote-source	Configure the source device for an RSPAN session.
monitor session remote-destination	Configure a destination device for an RSPAN session.
monitor session source interface	Configure the source port for a local SPAN session.
monitor session source vlan	Specify a VLAN as the data source of SPAN.
no monitor session	Delete all SPAN sessions.
remote-span	Configure a remote VLAN.
origin ip address	Configure a source IP address for GRE encapsulation.
show monitor	Display the SPAN sessions.
source interface	Configure a source port for ERSPAN.
shutdown	Shut down an ERSPAN session.
vrf	Associate a VRF with ERSPAN.

1.1 default monitor session

Function

Run the **default monitor session** command to delete all switch port analyzer (SPAN) sessions.

Syntax

default monitor session { *session-number* | **all** }

Parameter Description

session-number: ID of a SPAN session. The value range is from 1 to 4.

all: Indicates all SPAN sessions.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays SPAN sessions configured on the device.

```
Hostname> enable
Hostname# show running-config | include monitor session
monitor session 1 remote-source
monitor session 1 destination remote vlan 10 interface GigabitEthernet 0/1
monitor session 1 filter vlan 3 rx
```

The following example removes all the SPAN sessions from the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# default monitor session all
Hostname(config)# exit
Hostname# show running-config | include monitor session
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 destination ip address

Function

Run the **destination ip address** command to configure the destination IP address when the encapsulation type is GRE.

Run the **no** form of this command to remove this configuration.

By default, no destination IP address is configured when the encapsulation type is GRE.

Syntax

destination ip address *ipv4-address*

no destination ip address

Parameter Description

ipv4-address: Destination IP address when the encapsulation type is GRE.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the destination IP address to 10.1.1.2 when the SPAN encapsulation type is GRE.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# destination ip address 10.1.1.2
```

Notifications

When the entered IP address is invalid, the following notification will be displayed:

```
Invalid ip address
```

Platform Description

N/A

Common Errors

N/A

Related Commands

N/A

1.3 ip dscp

Function

Run the **ip dscp** command to configure the DSCP value for an encapsulated IP packet.

Run the **no** form of this command to restore the default DSCP value.

The default DSCP of the encapsulated IP packet is **0**.

Syntax

ip dscp *dscp-value*

no ip dscp

Parameter Description

dscp-value: DSCP value of the encapsulated IP packet. The value range is from 0 to 63.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the DSCP of the encapsulated IP packet to 56.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# ip dscp 56
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip ttl

Function

Run the **ip ttl** command to configure the TTL value for an encapsulated IP packet.

Run the **no** form of this command to restore the default TTL value.

The default TTL of the encapsulated IP packet is **64**.

Syntax

ip ttl *ttl-value*

no ip ttl

Parameter Description

ttl-value: TTL value of the encapsulated IP packet. The value range is from 1 to 255.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the TTL of the encapsulated IP packet to 65.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# ip ttl 65
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 mac-loopback

Function

Run the **mac-loopback** command to enable the MAC loopback function of an interface.

Run the **no** form of this command to disable this feature.

By default, MAC loopback is disabled for an interface.

Syntax

mac-loopback

no mac-loopback

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When configuring one-to-many SPAN, you need to use this command to enable the MAC loopback function of an interface.

Do not add other configurations for this interface.

To save port resources, you are advised to configure a port in Down state as the MAC loopback port.

Examples

The following example configures the remote VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 100
Hostname(config-vlan)# remote-span
Hostname(config-vlan)# exit
```

The following example configures a source device and configures GigabitEthernet 0/1 as the source port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 remote-source
Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1 both
```

The following example configures GigabitEthernet 0/2 as the destination port, and enables the MAC loopback function on this port. (You can see that the state of GigabitEthernet 0/2 changes to Up instantly.)

```
Hostname(config)# monitor session 1 destination remote vlan 100 interface
gigabitEthernet 0/2 switch
Hostname(config)# interface gigabitEthernet 0/2
```

```
Hostname(config-if-GigabitEthernet 0/2)# switchport access vlan 100
Hostname(config-if-GigabitEthernet 0/2)# mac-loopback
```

The following example adds GigabitEthernet 0/3-4 to remote VLAN 100.

```
Hostname(config)# interface range gigabitEthernet 0/3-4
Hostname(config-if-range)# switchport access vlan 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 monitor session destination interface

Function

Run the **monitor session destination interface** command to configure a destination port for a local SPAN session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no destination port is configured for a local SPAN session.

Syntax

monitor session *session-number* **destination interface** *interface-type interface-number* [**switch**]

no monitor session *session-number* **destination interface** *interface-type interface-number* [**switch**]

default monitor session *session-number* **destination interface** *interface-type interface-number* [**switch**]

Parameter Description

session-number: ID of a SPAN session.

interface-type interface-number: Type and number of the source or destination port.

switch: Configures the switching function of the destination port.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/AExamples

The following example configures GigabitEthernet 0/1 as the source port and GigabitEthernet 0/2 as the destination port for SPAN session 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1
Hostname(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

Notifications

On some devices that do not support configuration of SPAN for AP member ports, if you try to configure an AP member port as the source or destination port for SPAN, the following notification will be displayed:

```
Set fail on ap member.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 monitor session destination remote vlan interface

Function

Run the **monitor session destination remote vlan interface** command to configure an output port on an RSPAN source device or a destination port on an RSPAN destination device for an RSPAN session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no output port on the RSPAN source device or no destination port on the RSPAN destination device is configured.

Syntax

monitor session *session-number* **destination remote vlan** *remote-vlan-id* **interface** *interface-type interface-number* [**switch**]

no monitor session *session-number* **destination remote vlan** *remote-vlan-id* **interface** *interface-type interface-number* [**switch**]

default monitor session *session-number* **destination remote vlan** *remote-vlan-id* **interface** *interface-type interface-number* [**switch**]

Parameter Description

session-number: ID of a SPAN session.

interface-type interface-number: Type and number of the source or destination port.

remote-vlan-id: ID of a remote VLAN.

vlan-id-list: VLAN list (containing common VLANs instead of remote VLANs).

switch: Configures the switching function of the destination port.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures GigabitEthernet 0/1 as the output port on the source device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 remote-source
Hostname(config)# monitor session 1 destination remote vlan 10 interface
gigabitEthernet 0/1
```

Notifications

On some devices that do not support configuration of SPAN for AP member ports, if you try to configure an AP member port as the source or destination port for SPAN, the following notification will be displayed:

```
Set fail on ap member.
```

If the VLAN specified by remote-vlan-id does not exist or is not a remote VLAN, the following notification will be displayed:

```
vlan 1 doesn't exist or it isn't remote span vlan.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 monitor session erpsan-source

Function

Run the **monitor session erpsan-source** command to create an ERSPAN session.

Run the **no** form of this command to delete an ERSPAN session.

No ERSPAN session is created by default.

Syntax

monitor session *session-number* **erpsan-source**

no monitor session *session-number*

Parameter Description

session-number: ID of a SPAN session.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an ERSPAN session with the ID 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 erspan-source
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 monitor session filter vlan

Function

Run the **monitor session filter vlan** command to exclude one or more VLANs as the data source of SPAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no VLAN is excluded as the data source of SPAN.

Syntax

monitor session *session-number* **filter vlan** *vlan-id-list* **rx**

no monitor session *session-number* **filter vlan** *vlan-id-list* **rx**

default monitor session *session-number* **filter vlan** *vlan-id-list* **rx**

Parameter Description

session-number: ID of a SPAN session.

vlan-id-list: VLAN list (containing common VLANs instead of remote VLANs).

rx: **rx** indicates that only received packets are mirrored.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command must be configured together with the **monitor session source interface** command.

If you add or delete a VLAN source port to or from an effective SPAN session, you need to re-apply the entire SPAN session. Therefore, a few existing mirrored packets may be lost.

Examples

The following example excludes the RX direction of VLAN 2 as the data source of SPAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 filter vlan 2 rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **monitor session source interface**

1.10 monitor session remote-source

Function

Run the **monitor session remote-source** command to configure the source device for an RSPAN session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no source device is configured for an RSPAN session.

Syntax

monitor session *session-number* **remote-source**

no monitor session *session-number* **remote-source**

default monitor session *session-number* **remote-source**

Parameter Description

session-number: ID of a SPAN session.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the source device for the RSPAN session with ID 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 remote-source
```

Notifications

On some devices that do not support configuration of SPAN for AP member ports, if you try to configure an AP member port as the source or destination port for SPAN, the following notification will be displayed:

```
Set fail on ap member.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 monitor session remote-destination

Function

Run the **monitor session remote-destination** command to configure a destination device for an RSPAN session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no destination device is configured for an RSPAN session.

Syntax

monitor session *session-number* **remote-destination**

no monitor session *session-number* **remote-destination**

default monitor session *session-number* **remote-destination**

Parameter Description

session-number: ID of a SPAN session.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the destination device for the RSPAN session with ID 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 remote-destination
```

Notifications

On some devices that do not support configuration of SPAN for AP member ports, if you try to configure an AP member port as the source or destination port for SPAN, the following notification will be displayed:

```
Set fail on ap member.
```

If the VLAN specified by remote-vlan-id does not exist or is not a remote VLAN, the following notification will be displayed:

```
vlan 1 doesn't exist or it isn't remote span vlan.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 monitor session source interface

Function

Run the **monitor session source interface** command to configure the source port for a local SPAN session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no source port is configured for a local SPAN session.

Syntax

monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** [**acl** { *acl-name* | *acl-number* }] | **tx**]

no monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** [**acl** { *acl-name* | *acl-number* }] | **tx**]

default monitor session *session-number* **source interface** *interface-type interface-number* [{ **both** | **rx** [**acl** { *acl-name* | *acl-number* }] | **tx**]

Parameter Description

session-number: ID of a SPAN session.

interface-type interface-number: Type and number of the source port.

both: Indicates that both the received and sent packets are mirrored.

rx: Indicates that only the received packets are mirrored.

tx: Indicates that only the sent packets are mirrored.

acl { *acl-name* | *acl-number* }: Indicates that only packets that match ACL rules are mirrored. *acl-name*: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters. *acl-number*: Number of an ACL. For a standard IP ACL, the value range is from 1 to 99 and from 1300 to 1999. For an extended IP ACL, the value range is from 100 to 199 and from 2000 to 2699. For a MAC ACL, the value range is from 700 to 799.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If you do not specify **both**/**rx**/**tx** when configuring a source port, **both** is used by default. If the direction is specified, only packets in the specified direction are mirrored.

Examples

The following example configures GigabitEthernet 0/1 as the source port for SPAN session 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1
```

Notifications

On some devices that do not support configuration of SPAN for AP member ports, if you try to configure an AP member port as the source port for SPAN, the following notification will be displayed:

```
Set fail on ap member.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 monitor session source vlan

Function

Run the **monitor session source vlan** command to specify a VLAN as the data source of SPAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no VLAN is specified as the data source of SPAN.

Syntax

monitor session *session-number* **source vlan** *vlan-list* **rx**

no monitor session *session-number* **source vlan** *vlan-list* **rx** [**both** | **rx** | **tx**]

default monitor session *session-number* **source vlan** *vlan-list* **rx**

Parameter Description

session-number: ID of a SPAN session.

vlan-list: VLAN list (containing common VLANs instead of remote VLANs).

rx indicates that only received packets are mirrored.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If you add or delete a VLAN source port to or from an effective SPAN session, you need to re-apply the entire SPAN session. Therefore, a few existing mirrored packets may be lost.

Examples

The following example configures the RX direction of VLAN 2 as the data source of SPAN session 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 1 source vlan 2 rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 no monitor session

Function

Run the **no monitor session** command to delete all SPAN sessions.

Syntax

no monitor session { *session-number* | **all** }

Parameter Description

session-number: ID of a SPAN session. The value range is from 1 to 4.

all: Indicates all SPAN sessions.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays SPAN sessions configured on a device.

```
Hostname> enable
Hostname# show running-config | include monitor session
monitor session 1 remote-source
monitor session 1 destination remote vlan 10 interface GigabitEthernet 0/1
monitor session 1 filter vlan 3 rx
```

The following example deletes all SPAN sessions from the device.

```
Hostname# configure terminal
Hostname(config)# no monitor session all
Hostname(config)# exit
Hostname# show running-config | include monitor session
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 remote-span

Function

Run the **remote-span** command to configure a remote VLAN.

Run the **no** form of this command to remove this configuration.

By default, no remote VLAN is configured.

Syntax

remote-span

no remote-span

Parameter Description

N/A

Command Modes

VLAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures VLAN 100 as the remote VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 100
Hostname(config-vlan)# remote-span
```

Notifications

If this VLAN is already a remote VLAN, the following notification will be displayed when you run the **remote-span** command:

```
RSPAN vlan can't be set as remote span vlan.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 origin ip address

Function

Run the **origin ip address** command to configure a source IP address for GRE encapsulation.

Run the **no** form of this command to remove this configuration.

By default, no source IP address is configured for GRE encapsulation.

Syntax

origin ip address *ipv4-address*

no origin ip address

Parameter Description

ipv4-address: Source IP address specified for GRE encapsulation.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the source IP address of an IP packet to 11.1.1.2 when the ERSPAN encapsulation type is GRE.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# origin ip address 11.1.1.2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 show monitor

Function

Run the **show monitor** command to display the SPAN sessions.

Syntax

show monitor session *session-number*

Parameter Description

session *session-number*: Specifies the ID of a SPAN session.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all the SPAN sessions.

```
Hostname> enable
Hostname# show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2     frame-type Both
dest-intf:
GigabitEthernet 0/3
sess-num: 3
span-type: ERSPAN_SOURCE
src-intf:
```

```
 AggregatePort 1           frame-type: Both      TX status: Inactive   RX status:
Inactive
original ip address: 1.1.1.1
destination ip address: 1.1.1.2
status: disable
ip ttl: 64
ip dscp: 0
vrf: global-vrf
```

The following example displays the specified SPAN session.

```
Hostname> enable
Hostname# show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2     frame-type Both
dest-intf:
GigabitEthernet 0/3
```

Table 1-1 Output Fields of the show monitor Command

Field	Description
sess-num	ID of a SPAN session
span-type	SPAN type
src-intf	Source interface of the SPAN session
frame-type	Direction of streams to be mirrored
TX/RX status	Connectivity status of the route to the destination IP address when the ERSPAN session is valid (that is, the session is complete and not shut down): ● **Active**: The route to the destination IP address is reachable, and the ERSPAN session is active. ● **Inactive**: The route to the destination IP address is unreachable, and the ERSPAN session is inactive.
dest-intf	Destination interface of the SPAN session
original ip address	Source IP address for ERSPAN
destination ip address	Destination IP address for ERSPAN
status	Availability status of the ERSPAN session: ● **disable**: When the **shutdown** command is configured, the status is displayed as disable, and the session is unavailable. ● **enable**: The session is available.
ip ttl	TTL value of the encapsulated IP packet
ip dscp	DSCP value of the encapsulated IP packet

Field	Description
vrf	VRF information of the ESPAN session

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 source interface

Function

Run the **source interface** command to configure a source port for ERSPAN.
Run the **no** form of this command to remove this configuration.
By default, no source port is configured for ERSPAN.

Syntax

source interface *interface-type interface-numbere* [{ **both** | **rx** [**acl** { *acl-name* | *acl-number* }] | **tx**]

no source interface *interface-type interface-number* [{ **both** | **rx** [**acl** { *acl-name* | *acl-number* }] | **tx**]

Parameter Description

interface-type interface-number: Type and number of the source port.

both: Indicates that both the received and sent packets are mirrored.

rx: Indicates that only received packets are mirrored.

tx: Indicates that only the sent packets are mirrored.

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. For a standard IP ACL, the value range is from 1 to 99 and from 1300 to 1999. For an extended IP ACL, the value range is from 100 to 199 and from 2000 to 2699. For a MAC ACL, the value range is from 700 to 799.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

- When a sub-interface is configured as the source port, mirroring is supported only in the inbound direction.
- If you do not specify **both**/**rx**/**tx** when configuring a source port, **both** is used by default. If the direction is specified, only packets in the specified direction are mirrored.

Examples

The following example configures GigabitEthernet 0/1 as the source port for a stream-based ERSPAN session, and mirrors packets that match ACL 90.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# source interface gigabitEthernet 0/1 rx acl 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 shutdown

Function

Run the **shutdown** command to shut down an ERSPAN session.

Run the **no** form of this command to remove this configuration.

An ERSPAN session is enabled by default.

Syntax

no shutdown

Parameter Description

N/A

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example shuts down the ERSPAN session with ID 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 vrf

Function

Run the **vrf** command to associate a VRF with ERSPAN.

Run the **no** form of this command to remove this configuration.

By default, no VRF is associated with ERSPAN.

Syntax

vrf *vrf-name*

no vrf

Parameter Description

vrf-name: Name of a VRF.

Command Modes

ERSPAN configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example associates the VRF "vrf-name" with ERSPAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# monitor session 2 erspan-source
Hostname(config-mon-erspan-src)# vrf vrf-name
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 sFlow Commands

Command	Function
sflow agent	Configure the sFlow Agent address.
sflow collector destination	Configure the sFlow Collector address.
sflow collector max-datagram-size	Configure the maximum size of an output sFlow packet.
sflow counter collector	Configure the ID of the sFlow Collector for sFlow counter sampling.
sflow counter interval	Configure the interval for sFlow counter sampling.
sflow enable	Enable the sFlow function on an interface.
sflow flow collector	Configure the ID of the sFlow Collector for sFlow flow sampling.
sflow flow max-header	Configure the maximum length of the packet header copied during sFlow flow sampling.
sflow sampling-rate	Configure the sFlow flow sampling rate.
sflow source	Configure the source address of output sFlow packets.
show sflow	Display the sFlow configurations.

1.1 sflow agent

Function

Run the **sflow agent** command to configure the sFlow Agent address.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No sFlow Agent address is configured by default.

Syntax

sflow agent { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

no sflow agent { **address** | **interface** }

default sflow agent { **address** | **interface** }

Parameter Description

address { *ipv4-address* | **ipv6** *ipv6-address* }: Configures an IP address as the sFlow Agent address.

Here, *ipv4-address* indicates the IPv4 address of the sFlow Agent. **ipv6** *ipv6-address* indicates the IPv6 address of the sFlow Agent.

interface [**ipv6**] *interface-type interface-number*: Configures an interface as the sFlow Agent address.

Here, *interface-type interface-number* indicates the type and number of an interface configured with the IPv4 address. **ipv6** *interface-type interface-number* indicates the type and number of an interface configured with the IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the **Agent ip address** field in an output packet. If the sFlow Agent address is not configured, the packet cannot be output. The address must be a host IP address. If it is set to a non-host IP address, for example, a multicast or broadcast address, a notification indicating the configuration error is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.

Examples

The following example sets the sFlow Agent address to 192.168.2.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow agent address 192.168.2.1
```

Notifications

If an invalid address is configured, the following notification will be displayed:

```
invalid host address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 sflow collector destination

Function

Run the **sflow collector destination** command to configure the sFlow Collector address.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No sFlow Collector address is configured by default.

Syntax

sflow collector *collector-id* **destination** { *ipv4-address* | **ipv**6 *ipv6-address* } *udp-port-number* [**vrf** *vrf-name*] [**description** *collector-description*]

no sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6-ddress* } *udp-port-number* [**vrf** *vrf-name*] [**description** *collector-name*]

default sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6-address* } *udp-port-number* [**vrf** *vrf-name*] [**description** *collector-description*]

Parameter Description

collector-id: ID of the sFlow Collector. The value range is from 1 to 2.

ipv4-address: IPv4 address of the sFlow Collector.

ipv6 *ipv6-address*: Specifies the IPv6 address of the sFlow Collector.

udp-port-number: Number of a UDP port. The value range is from 1 to 65535.

vrf *vrf-name*: Specifies the name of a VRF instance.

description *collector-description*: Specifies the description of the sFlow Collector.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The sFlow Agent address must be a valid address. That is, the sFlow Agent address cannot be a multicast or broadcast address. It is recommended that the IP address of the sFlow Agent device be used.

- The sFlow Collector intercepts sFlow packets on the configured port.
- When the **vrf** parameter is configured, the corresponding VRF instance must be configured. If you configure a VRF instance for an sFlow Collector address and later remove this VRF instance, the sFlow Collector address will be removed as well.

Examples

The following example sets the address of sFlow Collector 1 to 192.168.2.100, listen port to 6343, and VRF instance name to vpn1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow collector 1 destination 192.168.2.100 6343 vrf vpn1
```

Notifications

If an invalid address is configured, the following notification will be displayed:

```
invalid host address.
```

If the VPN is not configured, the following notification will be displayed:

```
vpn is not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 sflow collector max-datagram-size

Function

Run the **sflow collector max-datagram-size** command to configure the maximum size of an output sFlow packet.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the maximum size of the output sFlow packet is **1400**.

Syntax

sflow collector *collector-id* **max-datagram-size** *datagram-size*

no sflow collector *collector-id* **max-datagram-size**

default sflow collector *collector-id* **max-datagram-size**

Parameter Description

collector-id: ID of the sFlow Collector. The value is 1 or 2.

max-datagram-size *datagram-size*: Specifies the maximum size of an output sFlow packet. The value range is from 200 to 9000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum size of an output sFlow packet to 1000 bytes for sFlow Collector 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow collector 1 max-datagram-size 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 sflow counter collector

Function

Run the **sflow counter collector** command to configure the ID of the sFlow Collector for sFlow counter sampling.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no ID of the sFlow Collector is configured for sFlow counter sampling.

Syntax

sflow counter collector *collector-id*

no sflow counter collector

default sflow counter collector

Parameter Description

collector-id: ID of the sFlow Collector. The value range is from 1 to 2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- You must configure an IP address for the sFlow Collector before the sFlow packets can be output.

Examples

The following example outputs the sFlow counter sampling packets on the port GigabitEthernet 0/1 to sFlow Collector 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# sflow counter collector 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 sflow counter interval

Function

Run the **sflow counter interval** command to configure the interval for sFlow counter sampling.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default interval for sFlow flow sampling is **30** seconds.

Syntax

sflow counter interval *sampling-interval-time*

no sflow counter interval

default sflow counter interval

Parameter Description

sampling-interval-time: Sampling interval, in seconds. The value range is from 3 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the global interval for sFlow counter sampling. This configuration applies to all interfaces.

Examples

The following example sets the global interval for sFlow counter sampling to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow counter interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 sflow enable

Function

Run the **sflow enable** command to enable the sFlow function on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The sFlow function is disabled by default.

Syntax

sflow enable [{ **ingress** | **egress** }

no sflow enable [{ **ingress** | **egress** }

default sflow enable [{ **ingress** | **egress** }

Parameter Description

ingress: Specifies inbound direction.

egress: Specifies outbound direction.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- This command can be configured on a physical or an aggregation port.
- If the direction is not specified, flow sampling is enabled in both the inbound and outbound directions.
- The counter sampling and flow sampling functions are enabled concurrently. Counter sampling is enabled when flow sampling is enabled in any direction of an interface.
- You must configure an IP address for the sFlow Collector before the sFlow packets can be output.
- The following configuration is not recommended because flow sample statistics may be inaccurate (for example, the configuration may not take effect, or statistics of an interface is displayed on another interface):
  - Flow sampling is enabled on an aggregation port and its member port.

Examples

The following example enables the sFlow function on the GigabitEthernet 0/1 port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# sflow enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 sflow flow collector

Function

Run the **sflow flow collector** command to configure the ID of the sFlow Collector for sFlow flow sampling.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no ID of the sFlow Collector is configured for sFlow flow sampling.

Syntax

sflow flow collector *collector-id*

no sflow flow collector

default sflow flow collector

Parameter Description

collector-id: ID the sFlow Collector. The value range is from 1 to 2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

-
- You must configure an IP address for the sFlow Collector before the sFlow packets can be output.

Examples

The following example outputs the sFlow flow sampling packets on the port GigabitEthernet 0/1 to sFlow Collector 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# sflow flow collector 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 sflow flow max-header

Function

Run the **sflow flow max-header** command to configure the maximum length of the packet header copied during sFlow flow sampling.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the maximum length of the packet header copied during sFlow flow sampling is **64**.

Syntax

sflow flow max-header *sampling-length*

no sflow flow max-header

default sflow flow max-header

Parameter Description

sampling-length: Maximum length of the packet header copied, in bytes. The value range is from 18 to 256.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of bytes that can be copied from the header of the original packet. The copied content is recorded in the generated sample. The protocol requires byte alignment during packet encapsulation, that is, the actual length of a sent packet is a multiple of 4. Therefore, the length of a collected packet may exceed the configured length. For example, when the maximum length is set to any of 21, 22, 23, and 24, the actual output packet length is 24.

Examples

The following example sets the maximum length of the packet header copied during sFlow flow sampling to 128 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow flow max-header 128
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 sflow sampling-rate

Function

Run the **sflow sampling-rate** command to configure the sFlow flow sampling rate.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default sFlow flow sampling rate is 65536.

Syntax

sflow sampling-rate *sampling-rate*

no sflow sampling-rate

default sflow sampling-rate

Parameter Description

sampling-rate: sFlow flow sampling rate, which indicates that a packet is sampled from every *sampling-rate* packets. The value is 65536.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the global flow sampling rate. This configuration applies to all interfaces.

Examples

The following example sets the sFlow flow sampling rate to **4096**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow sampling-rate 4096
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 sflow source

Function

Run the **sflow source** command to configure the source address of output sFlow packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the source address of output sFlow packets is the local device IP address which is used to ping the destination IP address.

Syntax

sflow source { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

no sflow source { **address** | **interface** }

default sflow source { **address** | **interface** }

Parameter Description

address { *ipv4-address* | **ipv6** *ipv6-address* }: Configures an IP address as the sFlow source address.

Here, *ipv4-address* indicates the IPv4 address of the sFlow source, which is not configured by default. **ipv6** *ipv6-address* indicates the IPv6 address of the sFlow source, which is not configured by default.

interface [**ipv6**] *interface-type interface-number*: Configures an interface as the sFlow source address.

interface-type interface-number indicates the type and number of an interface configured with the IPv4 address. **ipv6** *interface-type interface-number* indicates the type and number of an interface configured with the IPv6 address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure the source IP address of output packets.
- By default, the source address of output sFlow packets is the local device IP address which is used to ping the destination IP address.
- If the source interface is specified, the primary address (or the first global IPv6 address if any) of the interface is the source IP address of output packets.
- If the source interface is not specified, the default source address is used.

Examples

The following example sets the sFlow source address to 192.168.2.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sflow source address 192.168.2.1
```

Notifications

If an invalid address is configured, the following notification will be displayed:

```
invalid host address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show sflow

Function

Run the **show sflow** command to display the sFlow configurations.

Syntax

show sflow

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the sFlow configurations.

```
Hostname> enable
Hostname# show sflow
sFlow datagram version 5
Global information:
Agent IP: 10.10.10.10
sflow counter interval:30
sflow flow max-header:64
```

```
sflow sampling-rate:8192
Collector information:
ID   IP                      Port Size VPN
1    192.168.2.100             6343 1400
2    NULL                    0    1400
Port information
Interface                   CID  FID  Enable
TenGigabitEthernet 0/1        0    1    B
TenGigabitEthernet 0/2        0    1    N
```

Table 1-1 Output Fields of the show sflow Command

Field	Description
sFlow datagram version	sFlow packet version. The value is 5, indicating that only sFlow packets of version 5 can be sent.
Agent IP	IP address of the sFlow Agent
sflow counter interval	Counter sampling interval
sflow flow max-header	Maximum number of bytes that can be copied from the header of the original packet
sflow sampling-rate	Flow sampling rate
ID	sFlow Collector ID
IP	IP address of the sFlow Collector that receives the sFlow packets
Port	Port ID of the sFlow Collector that receives the sFlow packets
Size	Maximum size of the data part in an output sFlow packet
VPN	VPN instance name of the sFlow Collector
Interface	sFlow-enabled interface
CID	ID of the sFlow Collector to which the sFlow Agent outputs sFlow packets after counter sampling
FID	ID of the sFlow Collector to which the sFlow Agent outputs sFlow packets after flow sampling
Enable	Status of the sFlow function ● **B**: sFlow is enabled in both directions. ● **E**: sFlow is enabled in the outbound direction. ● **I**: sFlow is enabled in the inbound direction. ● **N**: sFlow is disabled.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Commands for Displaying Device Restart Reasons

Command	Function
show reboot-reason	Display the device restart reasons.

1.1 show reboot-reason

Function

Run the **show reboot-reason** command to display the device restart reasons.

Syntax

show reboot-reason [**all**]

Parameter Description

all: Displays restart reasons of all devices.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the device restart reasons.

```
Hostname> enable
Hostname# show reboot-reason all
Entry reboot information collecting begins, which may take some time.
Reboot information collecting end.
Slot 1/30, Cpu 0:
2019-08-14 05:58:39.254195 psh_toolkit:20041 reboot device. The reason is: self
healing.
Slot 1/31, Cpu 0:
2019-08-14 05:58:39.254195 psh_toolkit:20041 reboot device. The reason is: self
healing.
```

Table 1-1 Output Fields of the show reboot-reason all Command

Field	Description
Slot	Slot ID of a device or card
CPU	Sub-slot ID of a device or card

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 NTP Commands

Command	Function
no ntp	Disable the NTP synchronization with the time server, and clear all NTP configurations.
ntp access-group	Configure the NTP access control rights.
ntp authenticate	Configure the NTP global authentication mechanism.
ntp authentication-key	Configure an NTP global authentication key for the NTP service.
ntp disable	Disable the function of receiving NTP packets on an interface.
ntp discard	Configure the minimum packet request interval and average packet request interval allowed by NTP. The actual effective value is a power of 2.
ntp interval	Configure the interval for clock synchronization between the NTP client and NTP server.
ntp master	Configure the local clock as the NTP master clock to provide synchronization time for other devices.
ntp server	Specify an NTP server for an NTP client.
ntp service disable	Disable the NTP time synchronization service provided for other devices.
ntp trusted-key	Configure a key corresponding to an ID as a globally trusted key.
ntp update-calendar	Enable the NTP client to periodically update the hardware clock of the device using the clock synchronized from an external clock source.
show ntp server	Display the NTP server information.
show ntp status	Display the NTP information.
show ntp packets	Display information about the received and sent NTP packets.

1.1 no ntp

Function

Run the **no ntp** command to disable the NTP synchronization with the time server, and clear all NTP configurations.

The NTP service is disabled by default.

Syntax

no ntp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The NTP service is disabled by default. It is enabled only when the NTP server or NTP master clock is configured.

Examples

The following example disables the NTP service.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ntp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ntp access-group

Note

Whether a device supports this command depends on the ACL configuration.

Function

Run the **ntp access-group** command to configure the NTP access control rights.

Run the **no** form of this command to remove this configuration.

No NTP access control rule is configured by default.

Syntax

ntp access-group { **limited** | **peer** | **query-only** | **serve** | **serve-only** } *acl-number* | *acl-name* [**kod**]

no ntp access-group { **limited** | **peer** | **query-only** | **serve** | **serve-only** } *acl-number* | *acl-name*

Parameter Description

limited: Allows time request and control query for local NTP services, but limits the sending interval of request packets.

peer: Allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights).

query-only: Allows only control query for local NTP services.

serve: Allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system.

serve-only: Allows only time request for local NTP services.

acl-number: Number of an IP ACL. The value range is from 1 to 99 and from 1300 to 1999.

acl-name: Name of an IP ACL.

kod: If the KoD function is enabled in **limited** mode, the NTP server sends the corresponding KoD packet to the client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure the NTP access control rights of the local device. Access control provides a minimum security measure. A more secure method is to use the NTP authentication mechanism.
- When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is limited, peer, serve, serve-only, and query-only.
- If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.
- The system currently does not support the access control query function. Though rule matching is implemented in the preceding sequence, no request related to control query is supported.

Examples

The following example allows only the device with the IP address 192.168.1.1 to send a time request to a local device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.1.1
Hostname(config)# ntp access-group serve-only 1
```

The following example configures the NTP server, limits the request packet interval of the client, and sends KoD packets.

```
Hostname(config)# ip access-list standard limited 1
Hostname(config-std-nacl)# 10 permit any
Hostname(config-std-nacl)# exit
Hostname(config)# ntp access-group limited limited1 kod
Hostname(config)# ntp discard min-spacing 5 avg-spacing 5
Hostname(config)# ntp master
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ntp authenticate

Function

Run the **ntp authenticate** command to configure the NTP global authentication mechanism.

Run the **no** form of this command to remove this configuration.

The NTP global authentication mechanism is disabled by default.

Syntax

ntp authenticate

no ntp authenticate

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If no global security authentication mechanism is configured, synchronization communication is not encrypted. Encrypted communication with the server is initiated only when the global security authentication mechanism is enabled and the global key is configured.

Examples

The following example configures a global authentication key with the ID set to 6 and MD5 set to wooooop, specifies it as a globally entrusted key, and then enables the global authentication mechanism.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp authentication-key 6 md5 wooooop
Hostname(config)# ntp trusted-key 6
Hostname(config)# ntp authenticate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

1.4 ntp authentication-key

Function

Run the **ntp authentication-key** command to configure an NTP global authentication key for the NTP service.

Run the **no** form of this command to remove this configuration.

No authentication key is configured by default.

Syntax

ntp authentication-key *authentication-key-id* **md5** *authentication-key-string* [**0** | **7**]

no ntp authentication-key key-id

Parameter Description

authentication-key-id: ID of the key. The value range is from 1 to 4294967295.

authentication-key-string: Key string in text format. The maximum length of the key string is 31 bytes when the key is not encrypted, and 64 bytes when the key is encrypted.

0 | **7**: Indicates whether the key is encrypted. Here, **0** indicates no encryption, and **7** indicates simple encryption. The default value is **0**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure a global authentication key and use MD5 for encryption. Each key has a unique key-id. You can run the **ntp trusted-key** command to configure a key corresponding to key-id as a globally trusted key.
- You can configure up to 1024 keys, but a server supports only one key.

Examples

The following example configures an authentication key with the ID set to 6 and MD5 set to wooooop.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp authentication-key 6 md5 wooooop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ntp disable

Function

Run the **ntp disable** command to disable the function of receiving NTP packets on an interface.

The function of receiving NTP packets on an interface is enabled by default.

Syntax

ntp disable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- By default, NTP packets received on any interface can be provided for the client for clock adjustment. By configuring this command, you can disable the function of receiving NTP packets on the related interface to shield these packets.
- You can configure this command only on an interface that can be configured with an IP address.

Examples

The following example enables the function of receiving NTP packets on the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ntp disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ntp discard

Function

Run the **ntp discard** command to configure the minimum packet request interval and average packet request interval allowed by NTP. The actual effective value is a power of 2.

Run the **no** form of this command to remove this configuration.

By default, the minimum packet request interval allowed by NTP is 2s, and the average packet request interval is 8s.

Syntax

ntp discard min-spacing *discard-min-spacing-interval* **avg-spacing** *avg-spacing-interval*

no ntp discard

Parameter Description

discard-min-spacing-interval: Minimum interval at which the NTP client is allowed to send the request packet, in seconds. The actual interval is 2 to the power of *discard-min-spacing-interval*. The value range is from 1 to 8. The default value is **1**.

avg-spacing-interval: Average interval at which the NTP client is allowed to send the request packet, in seconds. The actual interval is 2 to the power of *avg-spacing-interval*. The value range is from 3 to 10. The default value is **3**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command must be used together with the **ntp access-group** { **limited** | **peer** | **serve** | **serve-only** | **query-only** } *acl-number* | *acl-name* [**kod**] command.
- The configured *discard-min-spacing-interval* and *avg-spacing-interval* are a power of 2, in seconds. For example, if *avg-spacing-interval* is set to 5, the actual average interval is 2 to the 5th power, that is, 32 seconds, instead of 5 seconds.
- When a KoD-enabled NTP device acts as a client, it reduces the rate after receiving a KoD packet. A KoD-disabled device does not reduce the rate.
- KoD cannot be triggered by specifying the interval in the **ntp interval** command.

Examples

The following example sets the minimum packet request interval allowed by NTP to 32s, and the average packet request interval to 32s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp discard min-spacing 5 avg-spacing 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ntp interval

Function

Run the **ntp interval** command to configure the interval for clock synchronization between the NTP client and NTP server.

Run the **no** form of this command to remove this configuration.

The interval for clock synchronization between the NTP client and NTP server is 64s by default.

Syntax

ntp interval *synchronization-interval-time*

no ntp interval

Parameter Description

synchronization-interval-time: Interval for clock synchronization, in seconds. The value range is from 10 to 2592000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The interval configured by this command does not take effect immediately. If you need this configuration to take effect immediately, enable NTP before configuring the interval.
- If the NTP client has not successfully synchronized the time, it quickly synchronizes the time at an interval of 5s. After the successful synchronization, the NTP server synchronizes the time at the configured interval.

Examples

The following example sets the interval for clock synchronization between the NTP client and NTP server to 1 hour.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp interval 3600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 ntp master

Caution

Use this command with caution. After a local clock is configured as the master clock (especially when a clock with a lower stratum is specified), a real effective clock source may be overwritten. If this command is used for

multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.

Function

Run the **ntp master** command to configure the local clock as the NTP master clock to provide synchronization time for other devices.

Run the **no** form of this command to remove this configuration.

The NTP master clock is disabled by default.

Syntax

ntp master [*stratum*]

no ntp master

Parameter Description

stratum: Stratum of the local clock. The value range is from 1 to 15. The default value is 8.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Before this command is configured, if this system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference.
- When the local system cannot synchronize time with the external clock source due to a network connection failure or other reasons, you can use this command to configure the local clock as the NTP master clock to provide synchronization time for other devices.
- After this command is executed, the system does not synchronize with a clock source with a higher stratum.

Examples

The following example configures the local clock as the NTP master clock and sets its stratum to 12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp master 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ntp server

Function

Run the **ntp server** command to specify an NTP server for an NTP client.

Run the **no** form of this command to remove this configuration.

No NTP server is configured by default.

Syntax

ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-address* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } [**key** *keyid*] [**prefer**] [**source** *interface-type interface-number*] [**version** *version*] [**via** *mgmt-name*]

no ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-address* | *ipv6-address* | **ip** *domain* | **ipv6** *domain* }

Parameter Description

oob: Accesses the NTP server through the MGMT port. By default, the local device does not access the NTP server through the MGMT port.

vrf *vrf-name*: Specifies the name of the VRF instance used to access the NTP server. By default, the VRF is not used to access the NTP server.

ipv4-address: IPv4 address of the NTP server.

ipv6-address: IPv6 address of the NTP server.

peer-hostname: Name of the server.

ip *domain*: Specifies the IPv4 domain name of the NTP server.

ipv6 *domain*: Specifies the IPv6 domain name of the NTP server.

key *keyid*: Specifies the key used for encrypted communication with the peer. The value range is from 1 to 4294967295. By default, the communication is not encrypted.

prefer: Specifies a server as the preferred server. No server is configured as the preferred server by default.

source *interface-type interface-number*: Specifies the type and number of the source interface (L3 interface) for sending the NTP packets. By default, a route is selected by the forwarding plane.

version *version*: Specifies the NTP version. The value range is from 1 to 4. By default, NTPv4 is used.

via *mgmt-name*: Specifies the egress port of packets in **oob** mode as the MGMT port.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The device supports up to 20 synchronization servers.
- You need to first configure a global encryption key and a globally trusted key, and then specify the keys as

the server trusted keys before the local device can initiate encrypted communication with the server. To implement encrypted communication with the server, ensure that the server has the same global encryption key and globally trusted key as the local device.

- If the precision is the same, the clock of the preferred server is selected for synchronization.
- When configuring the source interface for sending NTP packets, ensure that this interface is already configured with an IP address and can communicate with the corresponding NTP server.

Examples

The following example configures a device with the IP address 192.168.210.222 in the network as the NTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp server 192.168.210.222
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ntp service disable

Function

Run the **ntp service disable** command to disable the NTP time synchronization service provided for other devices.

Run the **no** form of this command to remove this configuration.

The NTP time synchronization service is enabled by default.

Syntax

ntp service disable

no ntp service disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If NTP works in client/server mode, after the NTP device synchronizes time from an external reliable clock source, the device acts as the time server to provide the time synchronization service for other devices. If you want the NTP device to act simply as a client, configure this command to disable the NTP time synchronization service.
- This command is mutually exclusive with the **ntp master** command. If the **ntp master** command is configured, the device acts as the server and the NTP time synchronization service cannot be disabled. If this command is configured, the **ntp master** command cannot be executed to configure the local clock as the NTP master clock.

Examples

The following example disables the NTP time synchronization provided for other devices.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp service disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ntp trusted-key

Function

Run the **ntp trusted-key** command to configure a key corresponding to an ID as a globally trusted key.

Run the **no** form of this command to remove this configuration.

No globally trusted key is configured by default.

Syntax

ntp trusted-key *trusted-key-id*

no ntp trusted-key *trusted-key-id*

Parameter Description

trusted-key-id: ID of a globally trusted key. The value range is from 1 to 4294967295.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

During NTP communication, two parties must use the same trusted key. To improve security, the key itself is not transmitted. Therefore, it is necessary to find the key based on the ID of the globally trusted key.

Examples

The following example configures an authentication key 6 as the key trusted by the corresponding server.

```
Hostname(config)# ntp authentication-key 6 md5 wooooop
Hostname(config)# ntp trusted-key 6
Hostname(config)# ntp server 192.168.210.222 key 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ntp update-calendar

Function

Run the **ntp update-calendar** command to enable the NTP client to periodically update the hardware clock of the device using the clock synchronized from an external clock source.

Run the **no** form of this command to remove this configuration.

By default, automatic update of the hardware clock is not configured on the NTP client.

Syntax

ntp update-calendar

no ntp update-calendar

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The hardware clock of the device can continue to work even when the device is shut down or reset.

Examples

The following example configures automatic update of the hardware clock by the NTP client.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ntp update-calendar
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show ntp server

Function

Run the **show ntp server** command to display the NTP server information.

Syntax

show ntp server

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

If the NTP service is configured, the current NTP server information is displayed; otherwise, the command does not print any information.

Examples

The following example displays the NTP server information of the current system.

```
Hostname> enable
Hostname# show ntp server
ntp-server                          source    keyid       prefer  version  status
10::2                              None      None        FALSE   4       candidate
192.168.210.222                     None      None        FALSE   4       select
```

Table 1-1 Output Fields of the show ntp server Command

Field	Description
ntp-server	IP address or domain name of the NTP server
source	Source interface of the NTP server
keyid	Key used for encrypted communication with the corresponding server
prefer	Whether the corresponding server is the preferred server
version	NTP version. The value range is from 1 to 4.
status	Status of the NTP server: ● select: status in which an optimal clock is finally selected ● candidate ● backup ● falseticker ● outlier ● excess ● reject

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show ntp status

Function

Run the **show ntp status** command to display the NTP information.

Syntax

show ntp status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command does not print any information before the synchronization server is added for the first time.

Examples

The following example displays the NTP information of the current system.

```
Hostname> enable
Hostname# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.000 Hz, actual freq is 250.000 Hz, precision is 2**23
reference time is E00DFF79.87EEFAD7 (02:29:13.000 UTC Wed, Feb 13, 2019)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.19760 msec, peer dispersion is 0.18751 msec
system poll interval is 64, last update was 6 sec ago
system time is E00DFF7F.E1BCFD4B (02:29:19.000 UTC Wed, Feb 13, 2019)
```

Table 1-2 Output Fields of the show ntp status Command

Field	Description
stratum	Stratum of the current clock
reference	Address of the synchronization server
freq	Clock frequency of the current system
precision	Clock precision of the current system
reference time	UTC time of the reference clock of the synchronization server
clock offset	Offset of the current clock
root delay	Delay of the current clock
root dispersion	Time precision of the root server
peer dispersion	Time precision of the synchronization server

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show ntp packets

Function

Run the **show ntp packets** command to display information about the received and sent NTP packets.

Syntax

show ntp packets

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the NTP information of the current system.

```
Hostname> enable
Hostname# show ntp packets
NTP Packet Statistical Information
Sent                         : 10
   Sent suceess               : 10
   Sent failures              : 0
Received                     : 10
   Recv processed             : 10
   Recv droped                : 0
       Authentication failures : 0
       Invalid packets         : 0
       Access denied           : 0
```

```
Interface disabled     : 0
Service disabled       : 0
Other reasons          : 0
```

Table 1-3 Output Fields of the show ntp packets Command

Field	Description
Sent success	Number of packets that are sent successfully
Sent failures	Number of packets that fail to be sent
Recv processed	Number of packets that are received and processed successfully
Recv dropped	Number of packets that are received but dropped
Authentication failures	Number of packets that are received but dropped due to authentication failures
Invalid packets	Number of packets that are received but dropped because the packets are invalid
Access denied	Number of packets that are received but dropped because these packets cannot be processed
Interface disabled	Number of packets that are received but dropped because processing of these packets is disabled on the interface
Service disabled	Number of packets that are dropped because the NTP service is disabled
Other reasons	Number of packets that are dropped due to other reasons

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 SNTP Commands

Command	Function
sntp enable	Enable the SNTP function.
sntp interval	Configure the interval for clock synchronization between the SNTP client and NTP/SNTP server.
sntp server	Configure an SNTP server.
show sntp	Display the SNTP information.

1.1 sntp enable

Function

Run the **sntp enable** command to enable the SNTP function.

Run the **no** form of this command to disable this feature.

The SNTP function is disabled by default.

Syntax

sntp enable

no sntp enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the SNTP function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sntp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 sntp interval

Function

Run the **sntp interval** command to configure the interval for clock synchronization between the SNTP client and NTP/SNTP server.

Run the **no** form of this command to remove this configuration.

The default interval for clock synchronization between the NTP client and NTP/SNTP server is 1800s.

Syntax

sntp interval *synchronization-interval-time*

no sntp interval

Parameter Description

synchronization-interval-time: Interval for clock synchronization, in seconds. The value range is from 60 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The interval configured by this command does not take effect immediately. If you need this configuration to take effect immediately, run the **sntp enable** command after configuring the interval.

Examples

The following example sets the SNTP time synchronization interval to 1 hour.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sntp interval 3600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 sntp server

Function

Run the **sntp server** command to configure an SNTP server.

Run the **no** form of this command to remove this configuration.

No SNTP server is configured by default.

Syntax

sntp server [**oob**] { *ipv4-address* | *domain* } [**source** *ipv4-address*] [**via** *mgmt-name*]

no sntp server

Parameter Description

oob: Accesses the SNTP server through the MGMT port. By default, the local device does not access the SNTP server through the MGMT port.

ipv4-address | *domain*: SNTP server. Here, *ipv4-address* indicates the IP address of the SNTP server, and *domain* indicates the domain name of the SNTP server.

source *ipv4-address*: Specifies the source IP address of SNTP.

via *mgmt-name*: Specifies the egress port of packets in oob mode as the MGMT port.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Since SNTP is fully compatible with NTP, the SNTP server can be configured as a public NTP server on the Internet.

Examples

The following example configures the device with the IP address 192.168.4.12 as an SNTP server in the network.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# sntp server 192.168.4.12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show sntp

Function

Run the **show sntp** command to display the SNTP information.

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the SNTP information.

```
Hostname> enable
Hostname# show sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

Table 1-1 Output Fields of the show sntpshow sntp Command

Field	Description
State	SNTP status
Server	Time synchronization server
sync interval	Time synchronization interval
Time zone	Current time zone

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 FTP Server Commands

Command	Function
clear ftp-server block-list	Clear the user lock entries in the FTP lock list.
ftp-server enable	Enable the FTP server.
ftp-server login timeout	Configure the FTP login timeout.
ftp-server login times	Configure the FTP login times.
ftp-server login permission enable	Enable read/write permission control of FTP users.
ftp-server login ip-block disable	Disable the IP address lock function.
ftp-server login username-block disable	Disable the username lock function.
ftp-server login silence-time	Configure the FTP lock time.
ftp-server login max-block-limit	Configure the maximum number of IP addresses that can be locked.
ftp-server topdir	Configure the top-level directory under which the FTP client can read and write files.
ftp-server timeout	Configure the idle timeout of an FTP session.
ftp-server username password	Configure the username and password for login to the FTP server.
ftp-server authentication	Enable AAA on the FTP server.
ftp-server max-sessions	Configure the maximum number of FTP sessions.
show ftp-server	Display status information of the FTP server.
show ftp-server list	Display the status information of FTP lock entries.

1.1 clear ftp-server block-list

Function

Run the **clear ftp-server block-list** command to clear the user lock entries in the FTP lock list.

Syntax

clear ftp-server block-list [**all** | **ip-address** { *ipv4-address* | *ipv6-address* } [**vrf** *vrf_name*] | **username** *user*]

Parameter Description

all: Clears all user lock entries in the FTP lock list.

ip-address: Clears a specified user lock entry based on the IP address.

ipv4-address: IPv4 address.

ipv6-address: IPv6 address.

vrf *vrf-name*: Specifies a VRF instance. If this parameter is not specified, the public network instance is used.

username *user*: Clears a specified user lock entry based on the username.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After the lock function is enabled, if a user has been locked because the number of his/her login failures reaches the upper limit, a lock entry is generated. This command can be used to delete a specified entry based on the IP address or username, or delete all lock entries.

When both the IP address lock and username lock functions are enabled, if you want to unlock a locally configured username, check whether the IP address is also locked. If the IP address is also locked, unlock the IP address as well so that the user can log in to the FTP server normally.

Examples

The following example clears specified lock entries based on the IPv4 address 1.1.1.1 and VRF name ftp-vrf.

```
Hostname> enable
Hostname# clear ftp-server lock-list ip-address 1.1.1.1 vrf ftp-vrf
```

The following example clears specified lock entries based on the username admin.

```
Hostname> enable
Hostname# clear ftp-server lock-list username admin
```

The following example clears all lock entries.

```
Hostname> enable
Hostname# clear ftp-server lock-list username all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server login ip-block disable**
- **ftp-server login username-block disable**

1.2 ftp-server enable

Function

Run the **ftp-server enable** command to enable the FTP server.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The FTP server is disabled by default.

Syntax

ftp-server enable

no ftp-server enable

default ftp-server enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the FTP server is enabled, you can connect to the FTP server through the FTP client and perform operations such as file upload or download.

The FTP client can access files on the FTP server only after this command and **ftp-server topdir** are configured.

Examples

The following example enables the FTP server, and allows the client to access only the **syslog** sub-directory.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server topdir /syslog
Hostname(config)# ftp-server enable
```

The following example disables the FTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server enable
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server topdir**

1.3 ftp-server login timeout

Function

Run the **ftp-server login timeout** command to configure the FTP login timeout.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the FTP login timeout is 2 minutes.

Syntax

ftp-server login timeout *time*

no ftp-server login timeout

default ftp-server login timeout

Parameter Description

time: FTP login timeout, in minutes. The value range is from 1 to 30.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The login timeout refers to the maximum time that the user can stay online after the username and password are verified. If the username and password are not verified again before login timeout, the session will be terminated to ensure that other users can log in to the FTP server.

Examples

The following example sets the FTP login timeout to 5 minutes.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ftp-server login timeout 5
```

The following example restores the default FTP login timeout to 2 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login timeout
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ftp-server login times

Function

Run the **ftp-server login times** command to configure the FTP login times.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the FTP login times is 3.

Syntax

ftp-server login times *times*

no ftp-server login times

default ftp-server times

Parameter Description

times: FTP login times. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The FTP login times refers to the maximum number of times that the user's account and password can be verified during FTP login. By default, the FTP login times is 3, that is, a session will be terminated once you enter an incorrect username or password so that other users can go online.

Examples

The following example sets the FTP login times to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login times 5
```

The following example restores the default FTP login times to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login times
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ftp-server login permission enable

Function

Run the **ftp-server login permission enable** command to enable read/write permission control of FTP users.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

By default, read/write permission control of FTP users is disabled.

Syntax

ftp-server login permission enable

no ftp-server login permission enable

default ftp-server login permission enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the read/write permission control function is enabled, the configured FTP user levels or AAA username levels can be used to control read/write permissions. For details about user levels and corresponding permissions, refer to the **ftp-server username password** command.

By default, all users have the read/write permissions. After permission control is enabled, if the user level is not configured, it is set to 1 by default and the user has only the read permission, that is, the user can only download data. You can configure FTP users of different levels as required for read/write permission control.

Examples

The following example enables read/write permission control of FTP users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login permission enable
```

The following example disables read/write permission control of FTP users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login permission enable
```

Notifications

N/A

Related Commands

- **ftp-server username password**

1.6 ftp-server login ip-block disable

Function

Run the **ftp-server login ip-block disable** command to disable the IP address lock function.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The IP address lock function is enabled by default.

Syntax

ftp-server login ip-block disable

no ftp-server login ip-block disable

default ftp-server login ip-block disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the IP address lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect username or password reaches the configured upper limit, the FTP session is terminated and the user's IP address is locked. In addition, all users cannot log in to the FTP server properly using this IP address or username.

Examples

The following example disables the IP address lock function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login ip-block disable
```

The following example enables the IP address lock function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login ip-block disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ftp-server login username-block disable

1.7 ftp-server login username-block disable

Function

Run the **ftp-server login username-block disable** command to disable the username lock function.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The username lock function is enabled by default.

Syntax

ftp-server login username-block disable

no ftp-server login username-block disable

default ftp-server login username-block disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the username lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect password reaches the configured upper limit, the FTP session is terminated and the username is locked. The user cannot log in to the FTP server, but other users are not affected.

After the username lock function is enabled, only a locally configured FTP username can be locked. If the entered username is not configured, the IP address is locked instead.

Examples

The following example disables the username lock function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login username-block disable
```

The following example enables the username lock function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login username-block disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server login ip-block disable**

1.8 ftp-server login silence-time

Function

Run the **ftp-server login silence-time** command to configure the FTP lock time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the FTP lock time is 5 minutes.

Syntax

ftp-server login silence-time *time*

no ftp-server login silence-time

default ftp-server login silence-time

Parameter Description

time: FTP lock time, in minutes. The value range is from 1 to 30.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The FTP lock time refers to the duration that a user needs to wait for automatic unlocking after the user is locked because the number of the user's login failures reaches the upper limit. The locked user can log in to the FTP server only after the login silence time expires.

Examples

The following example sets the FTP lock time to 15 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login silence-time 15
```

The following example restores the default FTP login timeout to 5 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login silence-time
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server login times**

1.9 ftp-server login max-block-limit

Function

Run the **ftp-server login max-block-limit** command to configure the maximum number of IP addresses that can be locked.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, up to 30 IP addresses can be locked.

Syntax

ftp-server login max-block-limit *limit*

no ftp-server login max-block-limit

default ftp-server login max-block-limit

Parameter Description

limit: Maximum number of IP addresses that can be locked. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the IP address lock function is enabled, if the number of locked IP addresses reaches the upper limit, the full lock function is enabled. By then, the FTP server no longer accepts the connection request from any user until the number of locked IP addresses is smaller than the upper limit.

Examples

The following example sets the maximum number of IP addresses that can be locked to 50.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server login max-block-limit 50
```

The following example restores the default maximum number of IP addresses that can be locked to 30.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server login max-block-limit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ftp-server topdir

Function

Run the **ftp-server topdir** command to configure the top-level directory under which the FTP client can read and write files.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no top-level directory under which the FTP client can read and write files is configured, that is, the client is prohibited from accessing any directory on the FTP server.

Syntax

ftp-server topdir { *directory* | **flash:** *directory* | **tmp:** *directory* | **usb0:** *directory* }

no ftp-server topdir

default ftp-server topdir

Parameter Description

directory: Top-level directory under which the FTP client can perform read/write operations.

flash: *directory*: Specifies the directory of the Flash memory.

tmp: *directory*: Specifies the directory of the temporary memory.

usb0: *directory*: Specifies the directory of the USB memory.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The top-level directory of the FTP server limits the range of directories that can be accessed by the FTP client after login. You must specify the correct top-level directory so that the FTP client can access files on the FTP server.

If this command is not configured, the FTP client cannot access any files or directories on the FTP server.

Examples

The following example limits the top-level directory under which the FTP client can read and write files, and allows the FTP client to access only the **syslog** sub-directory.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ftp-server enable
Hostname(config)# ftp-server topdir /syslog
```

The following example prohibits the FTP client from accessing any files on the FTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server topdir
```

Notifications

When no directory is configured, the following notification will be displayed:

```
%FTPSRV-USER: Haven't config topdir!
```

When a non-existing directory is configured, the following notification will be displayed:

```
Hostname(config)#ftp-server topdir ab
folder /ab don't exist!
```

Common Errors

- An invalid directory is configured.
- No directory is configured.

Platform Description

N/A

Related Commands

- **show ftp-server**

1.11 ftp-server timeout

Function

Run the **ftp-server timeout** command to configure the idle timeout of an FTP session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the idle timeout of an FTP session is 10 minutes.

Syntax

ftp-server timeout *time*

no ftp-server timeout

default ftp-server timeout

Parameter Description

time: Idle timeout, in minutes. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the FTP session idle timeout. If no operation is performed on the current session within the specified time (that is, the session is idle), the FTP server considers that the connection has failed and therefore releases the connection with the user.

The session idle timeout refers to the time from the completion of the last FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command (for example, after a file is completely transferred), the server starts to count the idle time again, and stops counting when the next FTP client command arrives. Therefore, the configuration of the idle timeout does not affect time-consuming file transfer operations.

Examples

The following example sets the idle timeout to 5 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server timeout 5
```

The following example restores the default FTP login timeout to 10 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server timeout
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ftp-server**

1.12 ftp-server username password

Function

Run the **ftp-server username password** command to configure the username and password for login to the FTP server.

Run the **no** form of this command to lift the restrictions on users who log in to the FTP server.

Run the **default** form of this command to restore the default configuration.

By default, no username and password are configured for login to the FTP server, that is, no login users are restricted.

Syntax

ftp-server username *username* [**privilege** *level*] **password** [*type*] *password*

no ftp-server username *username*

default ftp-server username *username*

Parameter Description

username: Username used for login. The value is a case-sensitive string of 1 to 64 characters, and no space is allowed in the middle of the string. The username may contain English letters, half-width numbers, and half-width symbols.

password: Password used for login. The password must contain letters or numbers. Spaces can appear before or after the password, but will be ignored. Spaces in the middle of the password are regarded as part of the password. A plain-text password is a string of 1 to 25 characters, and a cipher-text password is a string of 4 to 52 characters.

privilege *level*: Specifies the level of the login user, which is used to control the read/write permissions of the user. The value range is from 0 to 15, and the default value is **1**. The levels are consistent with those defined by AAA. The range from 0 to 5 indicates read only, the range from 6 to 10 indicates write only, and the range from 11 to 15 indicates read and write.

type: 0 indicates not encrypted, and 7 indicates encrypted.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You must configure a username and password for login to the FTP server to authenticate the client. The password and the user must be in one-to-one correspondence. The FTP server does not support login of anonymous users. If the username configuration is cleared, the FTP client cannot pass the authentication of the FTP server. The FTP client must provide both the correct username and password to log in to the FTP server.

You can configure at most 10 users for an FTP server.

A user with the read-only permission can only download files from the FTP server. A user with the write-only permission can only upload files to the server. A user with both the read and write permissions can upload and download files to or from the FTP server.

Examples

The following example sets the username to **user** and password to **pass** to log in to the FTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server username user password pass
```

The following example lifts the restrictions on users who log in to the FTP server.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# no ftp-server username user
```

The following example sets the username to **user**, password to **pass**, and user level to **11**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server username user privilege 11 password pass
```

Notifications

When a user tries to log in to the FTP server before a username is configured on the server, the following notification will be displayed:

```
%FTPSRV-USER: Haven't config username!
```

When the configured username is too long, the following notification will be displayed:

```
Hostname(config)#$sssssssssssssssssssssssssssssssssddddddddddddddd
Username abcdefghjijklnn,sssssssssssssssssssssssssssssssssssddddddddddddddd is
NULL or too long, max length is 64.
```

When a user tries to log in to the FTP server before a password is configured on the server, the following notification will be displayed:

```
%FTPSRV-PASS: Haven't config password!
```

When the configured cipher-text password is too short, the following notification will be displayed:

```
Hostname(config)#ftp-server username user password 7 2
Invalid encrypted password, min length is 4, max length is 52.
```

When the configured plain-text password is too long, the following notification will be displayed:

```
Hostname(config)#ftp-server username user password abcdefghijklmnopqrstuvwxyz
% Password is too long, max length is 25
```

Common Errors

- The configured username contains invalid characters, or is too long.
- A user tries to log in to the FTP server before a username is configured on the server.
- A user tries to log in to the FTP server before a password is configured on the server.
- The configured password is too short or too long.
- The password contains invalid characters.

Platform Description

N/A

Related Commands

- **show ftp-server**

1.13 ftp-server authentication

Function

Run the **ftp-server authentication** command to enable AAA on the FTP server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, FTP does not support AAA login authentication.

Syntax

ftp-server authentication { **default** | *name* }

no ftp-server authentication

default ftp-server authentication

Parameter Description

default: Uses the default authentication mode in the AAA configuration.

name: Specified name in the AAA configuration.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command takes effect only after FTP is enabled.

Enable the AAA function before configuring this command.

Examples

The following example enables AAA on the FTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server enable
Hostname(config)# ftp-server topdir tmp:
Hostname(config)# ftp-server authentication 111
Hostname(config)# aaa new-model
Hostname(config)# aaa authentication ftp 111 local
```

Related Commands

- **ftp-server topdir**
- **aaa new-model** (Security/AAA)
- **aaa authentication ftp** (Security/AAA)

1.14 ftp-server max-sessions

Function

Run the **ftp-server max-sessions** command to configure the maximum number of FTP sessions.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the maximum number of FTP sessions is 20.

Syntax

ftp-server max-sessions *session*

no ftp-server max-sessions

default ftp-server max-sessions

Parameter Description

session: Maximum number of user connections allowed. The value range is from 1 to 20.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The maximum number of FTP sessions refers to the maximum number of users that can be concurrently connected to the FTP server. The default value is 20. That is, if the number of FTP sessions reaches 20, no more user can log in to the FTP server unless a session is closed.

Examples

The following example sets the maximum number of FTP sessions to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-server max-sessions 5
```

The following example restores the default maximum number of FTP sessions to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ftp-server max-sessions
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 show ftp-server

Function

Run the **show ftp-server** command to display status information of the FTP server.

Syntax

show ftp-server

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display status information of the FTP server, including the server startup status, top-level directory, and user information (username, password, and number of connections) of the FTP server. If a connection is configured, the following information is also displayed: IP address, port, transmission type, and active or passive mode.

Examples

The following example displays status information of the FTP server.

```
Hostname> enable
Hostname# show ftp-server
   ftp-server information
==================================
enable : Y
topdir : tmp:/
timeout: 10min
username:aaaa        password:(PLAINT)bbbb        connect num[2]
  [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]
                        client IP:192.168.21.26[3927]
  [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
                        client IP:192.168.21.26[3929]
username:a1          password:(PLAINT)bbbb        connect num[0]
username:a2          password:(PLAINT)bbbb        connect num[0]
username:a3          password:(PLAINT)bbbb        connect num[0]
username:a4          password:(PLAINT)bbbb        connect num[0]
username:a5          password:(PLAINT)bbbb        connect num[0]
username:a6          password:(PLAINT)bbbb        connect num[0]
username:a7          password:(PLAINT)bbbb        connect num[0]
username:a8          password:(PLAINT)bbbb        connect num[0]
username:a9          password:(PLAINT)bbbb        connect num[0]
```

Table 1-1 Output Fields of the show ftp-server Command

Field	Description
enable	Whether the function is enabled

Field	Description
topdir	Top-level directory
timeout	Login timeout
username	Username
password	Password
connect num	Current number of client connections
trans-type	Transmission type
BINARY	Binary transmission mode
ASCII	Text transmission mode
server IP	IP address of the server
client IP	IP address of the client

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show ftp-server list

Function

Run the **show ftp-server list** command to display the status information of FTP lock entries.

Syntax

show ftp-server { **ip-block** | **username-block** } **list**

Parameter Description

ip-block: Displays the IP address of the lock entry.

username-block: Displays the username of the lock entry.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

FTP lock entries are classified into two types:

- IP address lock entries, which contain the following information: locked IP address, VRF name, and remaining time for unlocking.
- Username lock entries, which contain the following information: locked username and remaining time for unlocking.

Examples

The following example displays the IP address lock entries.

```
Hostname> enable
Hostname# show ftp-server ip-block list
---------------------------------------
Address                                              VRF Name
Unlock Interval(seconds)
---------------------------------------
172.30.33.50                                          default
1720
```

Table 1-2 Output Fields of the show ftp-server ip-block list Command

Field	Description
Address	Locked IP address
VRF Name	Name of the VRF where the locked IP address resides. The default value is **default**.
Unlock Interval(seconds)	Remaining time for unlocking, in seconds

The following example displays the username lock entries.

```
Hostname> enable
Hostname# show ftp-server username-block list
------------------------------
Username                                          Unlock Interval(seconds)
------------------------------
admin                                            1720
```

Table 1-3 Output Fields of the show ftp-server username-block list Command

Field	Description
Username	Locked username

Field	Description
Unlock Interval(seconds)	Remaining time for unlocking, in seconds

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ftp-server login ip-block disable**
- **ftp-server login username-block disable**

1 FTP Client Commands

Command	Function
ftp-client ascii	Set the FTP transmission mode to ASCII.
ftp-client disable-size-check	Disable the size check of files downloaded from the FTP server.
ftp-client port	Set the FTP data connection mode to PORT.
ftp-client source	Bind a source IP address to the FTP client.
copy ftp	Use the FTP client to download files from the FTP server to the local device.
copy flash	Use the FTP client to upload files from the local device to the server.
show ftp-client	Display information about the FTP client.

1.1 ftp-client ascii

Function

Run the **ftp-client ascii** command to set the FTP transmission mode to ASCII.

Run the **no** form of this command to set the FTP transmission mode to Binary.

Run the **default** form of this command to restore the default configuration.

The default FTP transmission mode is Binary.

Syntax

ftp-client [**vrf** *vrf-name*] **ascii**

no ftp-client [**vrf** *vrf-name*] **ascii**

default ftp-client [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Specifies a VRF instance. If this parameter is not specified, it indicates the public network instance.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To specify the **vrf** *vrf-name* parameter, configure the VRF first. For details about the VRF, see *Configuring VRF*.

Caution

When the **default ftp-client** command is configured, all the configurations of the FTP client are restored to the default configurations. That is, the data connection mode is PASV, the FTP transmission mode is Binary, and the client is not bound to any source IP address.

Examples

The following example sets the FTP transmission mode to ASCII.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-client ascii
```

Notifications

If the configuration succeeds, no notification will be displayed.

If the specified *vrf-name* is not configured on the local device, the following notification will be displayed:

```
% VPN Routing/Forwarding instance name error
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf** (IP routing/VRF)

1.2 ftp-client disable-size-check

Function

Run the **ftp-client disable-size-check** command to disable the size check of files downloaded from the FTP server.

Run the **no** form of this command to enable size check of files downloaded from the FTP server.

Run the **default** form of this command to restore the default configuration.

By default, the sizes of files downloaded from the FTP server are checked.

Syntax

ftp-client disable-size-check

no ftp-client disable-size-check

default ftp-client disable-size-check

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the FTP client downloads a file, it checks the file size by default to detect file transfer errors (if any). You can also disable the file size check when downloading files from FTP servers that cannot reply to FTP clients with file sizes.

Examples

The following example disables the size check of files downloaded from the FTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-client disable-size-check
```

Notifications

If the configuration succeeds, no notification will be displayed.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ftp-client port

Function

Run the **ftp-client port** command to set the FTP data connection mode to PORT.

Run the **no** form of this command to set the FTP data connection mode to PASV.

Run the **default** form of this command to restore the default configuration.

The default FTP data connection mode is PASV.

Syntax

ftp-client [**vrf** *vrf-name*] **port**

no ftp-client [**vrf** *vrf-name*] **port**

default ftp-client [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Specifies a VRF instance. If this parameter is not specified, it indicates the public network instance.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to set the FTP connection mode to PORT, in which the FTP server initiates a connection request to the client.

To specify the **vrf** *vrf-name* parameter, configure the VRF first. For details about the VRF, see "Configuring VRF" in "IP Routing."

Caution

When the **default ftp-client** command is configured, all the configurations of the FTP client are restored to the default configurations. That is, the data connection mode is PASV, the FTP transmission mode is Binary, and the client is not bound to any source IP address.

Examples

The following example enables the FTP client to set up the data connection in PORT mode based on vrf-name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-client vrf vrf-name port
```

Notifications

If the configuration succeeds, no notification will be displayed.

If the specified *vrf-name* is not configured on the local device, the following notification will be displayed:

```
% VPN Routing/Forwarding instance name error
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf** (IP routing/VRF)

1.4 ftp-client source

Function

Run the **ftp-client source** command to bind a source IP address to the FTP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no source IP address is bound to the FTP client. Instead, a source IP address is selected based on the route.

Syntax

ftp-client [**vrf** *vrf-name*] **source** { *ipv4-address* | *ipv6-address* | *interface-type interface-number* }

no ftp-client [**vrf** *vrf-name*] **source**

default ftp-client [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Specifies a VRF instance. If this parameter is not specified, it indicates the public network instance.

ipv4-address: Source IP address of the client.

ipv6-address: Source IPv6 address of the client.

interface-type interface-number: Type and number of the source interface of the client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to bind a source IP address to the FTP client so that the client can use this IP address to communicate with the server.

To specify the **vrf** *vrf-name* parameter, configure the VRF first. For details about the VRF, see "Configuring VRF" in "IP Routing."

Caution

When the **default ftp-client** command is configured, all the configurations of the FTP client are restored to the default configurations. That is, the data connection mode is PASV, the FTP transmission mode is Binary, and the client is not bound to any source IP address.

Examples

The following example binds the source IP address 192.168.23.236 to the FTP client vrf-name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-client vrf vrf-namesource 192.168.23.236
```

The following example binds the IP address of the source interface tenGigabitEthernet 1/0/1 to the FTP client vrf-name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ftp-client source tengigabitethernet 1/0/1
```

Notifications

If the configuration succeeds, no notification will be displayed.

If the bound IP address is not a local address, the following notification will be displayed:

```
Bind failed: the specified source address is non-local ip
```

If the specified *vrf-name* is not configured on the local device, the following notification will be displayed:

```
% VPN Routing/Forwarding instance name error
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip vrf** (IP routing/VRF)

1.5 copy ftp

Function

Run the **copy ftp** command to use the FTP client to download files from the FTP server to the local device.

Syntax

copy { **ftp: | oob_ftp:** } ***//****username****:****password****@****destination-ip-address* [***/****remote-directory*] ***/****remote-file* **flash:** [*local-directory****/***] *local-file*

Parameter Description

oob_ftp: Transfers files through the MGMT port.

username: Username for login to the FTP server. It is a string of 1 to 64 characters. The value cannot contain characters such as colon (:), at sign (@), slash (/) and spaces, and must be specified.

password: Password for login to the FTP server. It is a string of 1 to 64 characters. The value cannot contain characters such as colon (:), at sign (@), slash (/) and spaces, and must be specified.

destination-ip-address: IP address of the FTP server.

remote-directory: Directory on the FTP server, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working path of the FTP server is used.

remote-file: File name on the remote server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

flash: Indicates flash memory.

local-directory: Directory on the local device, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used.

local-file: Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

You can run the **dir** command to check whether the downloaded file is configured on the local device. If the file is configured, the download is successful; otherwise, the download fails.

Examples

The following example uses the username **user** and password **pass** to log in to the FTP server, downloads the **remote-file** file from the **root** directory of the FTP server with the IP address 192.168.23.69 to the **home** directory of the local device, and renames this file **local-file**.

```
Hostname> enable
Hostname# copy ftp://user:pass@192.168.23.69/root/remote-file flash:home/local-file
```

Notifications

If the download succeeds, the following notification will be displayed:

```
success
```

If the download fails, you can find the corresponding error message after running the **debug ftp-client** command.

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (Basic Configuration/File System Management)

1.6 copy flash

Function

Run the **copy flash** command to use the FTP client to upload files from the local device to the server.

Syntax

copy flash: [*local-directory***/**] *local-file* { **ftp: | oob_ftp:** } ***//****username***:***password@destination-ip-address* [***/****remote-directory*] ***/****remote-file*

Parameter Description

local-directory: Directory on the local device, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used.

local-file: Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

oob_ftp: Transfers files through the MGMT port.

username: Username for login to the FTP server. It is a string of 1 to 64 characters. The value cannot contain characters such as colon (:), at sign (@), slash (/) and spaces, and must be specified.

password: Password for login to the FTP server. It is a string of 1 to 64 characters. The value cannot contain characters such as colon (:), at sign (@), slash (/) and spaces, and must be specified.

destination-ip-address: IP address of the FTP server.

remote-directory: Directory on the FTP server, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working path of the FTP server is used.

remote-file: File name on the remote server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

You can run the **dir** command to check whether the uploaded file is configured on the FTP server. If the file is configured, the upload is successful; otherwise, the upload fails.

Examples

The following example uses the username **user** and password **pass** to log in to the FTP server, uploads the **local-file** file in the **home** directory of the local device to the **root** directory of the FTP server with the IP address 192.168.23.69, and renames the file **remote-file**.

```
Hostname> enable
Hostname# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

Notifications

If the upload succeeds, the following notification will be displayed:

```
success
```

If the upload fails, you can find the corresponding error message after running the **debug ftp-client** command.

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (Basic Configuration/File System Management)

1.7 show ftp-client

Function

Run the **show ftp-client** command to display information about the FTP client.

Syntax

show ftp-client

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about the FTP client, including the transmission type, and PASV or PORT mode.

Examples

The following example displays the information about the FTP client.

```
Hostname> enable
Hostname# show ftp-client
      ftp-client information
==================================
type: BINARY
mode: PASV
```

Table 1-1 Output Fields of the show ftp-client Command

Field	Description
type	Transmission type: ● Binary ● ASCII: text transmission
mode	Connection mode: ● PASV ● PORT

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 TFTP Server Commands

Command	Function
tftp-server enable	Enable the TFTP server.
tftp-server topdir	Configure the top-level directory under which the TFTP client can read and write files.
show tftp-server	Display the configurations of the current TFTP server.
show tftp-server updating-list	Display the file download progress of the current TFTP client.

1.1 tftp-server enable

Function

Run the **tftp-server enable** command to enable the TFTP server.

Run the **no** form of this command to disable the TFTP server.

The TFTP server is disabled by default.

Syntax

tftp-server enable

no tftp-server enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the TFTP server is enabled, files can be transmitted only through the MGMT port.

The TFTP client can access files on the TFTP server only after this command and **tftp-server topdir** are configured.

The TFTP server can connect to a maximum of 10 clients concurrently.

Examples

The following example enables the TFTP server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tftp-server enable
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **tftp-server topdir**
- **show tftp-server**

1.2 tftp-server topdir

Function

Run the **tftp-server topdir** command to configure the top-level directory under which the TFTP client can read and write files.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

By default, the TFTP client can read and write files in the Flash directory.

Syntax

tftp-server topdir *directory*

no tftp-server topdir

default tftp-server topdir

Parameter Description

directory: Top-level directory under which the TFTP client can perform read/write operations. Here, a slash (/) indicates the root directory.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The top-level directory of the TFTP server limits the range of directories that can be accessed by the TFTP client after login. You must specify the correct top-level directory so that the TFTP client can access files on the TFTP server.

Examples

The following example enables the TFTP server, and allows the client to access only the **Syslog** sub-directory.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tftp-server topdir /syslog
Hostname(config)# tftp-server enable
```

Notifications

When a non-existing directory is configured, the following notification will be displayed:

```
% topdir /ab don't exist!
```

When an invalid directory is configured, the following notification will be displayed:

```
% Root dir too long, max length is 64.
```

Common Errors

- A non-existing directory is configured.

- An invalid directory is configured.

Platform Description

N/A

Related Commands

- **tftp-server enable**
- **show tftp-server**

1.3 show tftp-server

Function

Run the **show tftp-server** command to display the configurations of the current TFTP server.

Syntax

show tftp-server

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to check the TFTP server enabling status and the top-level directory.

Examples

The following example displays the TFTP server configurations.

```
Hostname> enable
Hostname# show tftp-server
   tftp-server information
==================================
enable : Y
topdir : flash:/
```

Table 1-1 Output Fields of the show tftp-server Command

Field	Description
enable	Whether the TFTP server is enabled
topdir	Top-level directory configured for the TFTP server

Notifications

N/A

Platform Description

N/A

Related Commands

- **tftp-server enable**
- **tftp-server topdir**

1.4 show tftp-server updating-list

Function

Run the **show tftp-server updating-list** command to display the file download progress of the current TFTP client.

Syntax

show tftp-server updating-list

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the file download progress on the TFTP client.

```
Hostname> enable
Hostname# show  tftp-server updating-list
IP Address            Interface             File Name               TX
Elapsed
--------  --------  --------  ----  ----
171.208.208.2          Mgmt 0               main_map552.bin           6.28392%
00:00:05
```

Table 1-2 Output Fields of the show tftp-server updating-list Command

Field	Description
IP Address	IP address of the TFTP client

Field	Description
Interface	Name of the MGMT interface used by the TFTP client for download
File Name	File name requested by the TFTP client
TX	Current file download progress of the TFTP client
Elapsed	Time spent for download on the TFTP client

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1 TFTP Client Commands

Command	Function
tftp-client source	Bind a source IP address to the TFTP client.
copy tftp	Use the TFTP client to download files from the TFTP server to the local device.
copy flash	Use the TFTP client to upload files from the local device to the server.

1.1 tftp-client source

Function

Run the **tftp-client source** command to bind a source IP address to the TFTP client.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, no source IP address is bound to the TFTP client. Instead, a source IP address is selected based on the route.

Syntax

tftp-client source { **ip** *ipv4-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }

no tftp-client source

default tftp-client source

Parameter Description

ipv4-address: IPv4 address.

ipv6-address: IPv6 address.

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to bind a source IP address to the TFTP client so that the client can use this IP address to communicate with the server.

Examples

The following example binds the source IP address 192.168.23.236 to the TFTP client.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# tftp-client source ip 192.168.23.236
```

Notifications

If the configuration succeeds, no notification will be displayed.

If the configured IP address is not a local address, the following notification will be displayed:

```
Bind failed: the specified source address is non-local ip
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 copy tftp

Function

Run the **copy tftp** command to use the TFTP client to download files from the TFTP server to the local device.

Syntax

copy { **tftp:** | **oob_tftp:** } ***//****destination-ip-address* [***/****remote-directory*] ***/****remote-file* **flash:** [*local-directory****/***] *local-file*

Parameter Description

oob_tftp: Transfers files through the MGMT port.

destination-ip-address: IP address of the destination TFTP server.

remote-directory: Directory on the TFTP server, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working directory of the TFTP server is used.

remote-file: File name on the remote server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

flash: Indicates flash memory.

local-directory: Directory on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used.

local-file: Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

You can run the **dir** command to check whether the downloaded file is configured on the local device. If the file is configured, the download is successful; otherwise, the download fails.

Examples

The following example downloads the **remote-file** file from the **root** directory of the TFTP server with the IP address 192.168.23.69 to the **Flash** directory on the local device, and saves the file as **local-file**.

```
Hostname> enable
Hostname# copy tftp://192.168.23.69/root/remote-file flash:local-file
```

Notifications

If the download succeeds, the following notification will be displayed:

```
success
```

If the download fails, you can find the corresponding error message after running the **debug tftp** command.

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (Basic Configuration/File System Management)

1.3 copy flash

Function

Run the **copy flash** command to use the TFTP client to upload files from the local device to the server.

Syntax

copy flash: [*local-directory**/***] *local-file* { **tftp: | oob_tftp:** } ***//****destination-ip-address* [***/****remote-directory*] ***/****remote-file*

Parameter Description

oob_tftp: Transfers files through the MGMT port.

destination-ip-address: IP address of the destination TFTP server.

remote-directory: Directory on the TFTP server, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working directory of the TFTP server is used.

remote-file: File name on the remote server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

local-directory: Directory on the local device, which is optional. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used.

local-file: Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

You can run the **dir** command to check whether the uploaded file is configured on the TFTP server. If the file is configured, the upload is successful; otherwise, the upload fails.

Examples

The following example uploads the **local-file** file in the **Flash** directory on the device to the **root** directory of the TFTP server with an IP address 192.168.23.69, and renames the file **remote-file**.

```
Hostname> enable
Hostname# copy flash:local-file tftp://192.168.23.69/root/remote-file
```

Notifications

If the download succeeds, the following notification will be displayed:

```
success
```

If the download fails, you can find the corresponding error message after running the **debug tftp** command.

Common Errors

N/A

Platform Description

N/A

Related Commands

- **dir** (Basic Configuration/File System Management)

1 SNMP Commands

Command	Function
clear snmp locked-ip	Clear the list of source IP addresses that are locked after Simple Network Management Protocol (SNMP) authentication fails consecutively.
no snmp-server	Disable the SNMP agent function of a device.
show snmp	Display the SNMP status.
snmp trap link-status	Send a Link Trap message through an interface.
snmp-server authentication attempt	Configure the maximum number of consecutive SNMP authentication failures and specify the corresponding processing actions.
snmp-server chassis-id	Configure a system serial number.
snmp-server community	Configure an authentication name and access permission.
snmp-server contact	Configure a system contact mode.
snmp-server enable secret-dictionary-check	Configure password dictionary check for communities and users.
snmp-server enable traps	Enable the agent to actively send Trap messages to the NMS.
snmp-server enable version	Configure an SNMP version.
snmp-server flow-control pps	Configure SNMP traffic control.
snmp-server group	Configure an SNMP user group.
snmp-server host	Configure NMS host addresses for the agent to send messages.
snmp-server inform	Configure Inform message sending attempts and timeout time.
snmp-server location	Configure a system location.
snmp-server logging	Enable the SNMP logging function.
snmp-server net-id	Configure NE code information of a device.
snmp-server packetsize	Configure the maximum packet length of the SNMP agent.

snmp-server queue-length	Configure the queue of the Trap messages.
snmp-server source-interface	Configure the source port of a device to receive SNMP packets.
snmp-server system-shutdown	Enable the SNMP system reboot notification function.
snmp-server trap-format private	Include private fields in SNMP Trap messages.
snmp-server trap-source	Configure a source address for sending Trap messages.
snmp-server trap-timeout	Configure the timeout time of Trap message re-sending.
snmp-server udp-port	Configure the ID of a port that receives SNMP packets.
snmp-server user	Configure an SNMP user.
snmp-server view	Configure an SNMP view.

1.1 clear snmp locked-ip

Function

Run the **clear snmp locked-ip** command to clear the list of source IP addresses that are locked after Simple Network Management Protocol (SNMP) authentication fails consecutively.

Syntax

clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Parameter Description

ipv4 *ipv4-address*: Specifies the source IPv4 address to be cleared.

ipv6 *ipv6-address*: Specifies the source IPv6 address to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

- This command is used to manually clear source IP addresses that are locked after authentication fails consecutively. A list of source IP addresses or a specific source IP address can be cleared.
- After a source IP address is cleared, a request to authenticate the IP address can be initiated when SNMP access packets from this cleared IP address are received.

Examples

The following example clears the list of source IP addresses that are locked after SNMP authentication fails consecutively.

```
Hostname> enable
Hostname# clear snmp locked-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 no snmp-server

Function

Run the **no snmp-server** command to disable the SNMP agent function of a device.

The SNMP agent function is enabled by default.

Syntax

no snmp-server

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The SNMP agent function is enabled by default. When SNMP agent parameters (for example, Network Management System (NMS) host address, authentication name, and access permission) are configured, the SNMP agent service is automatically enabled. This command can be used to disable the agent service of all SNMP versions supported on a device.
- This command must be used with the **enable service snmp-agent** command to make the SNMP agent service take effect. Otherwise, the SNMP agent service will not take effect.
- After this command is run, all SNMP agent service configurations are shielded. In this case, running the **show running-config** will not display the configurations. The configurations can be restored after the SNMP agent service is enabled again. Running the **no enable service snmp-agent** will not shield the SNMP agent configurations.

Examples

The following example disables the SNMP agent service function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no snmp-server
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable service snmp-agent** (basic configuration/basic management)

1.3 show snmp

Function

Run the **show snmp** command to display the SNMP status.

Syntax

show snmp [**group** | **host** | **locked-ip** | **mib** | **process-mib-time** | **user** | **version** | **view**]

Parameter Description

group: Displays SNMP user group information.

host: Displays user configuration information.

locked-ip: Displays source IP address that is locked after consecutive SNMP authentication failure.

mib: Displays SNMP management information base (MIB) information supported in the system.

process-mib-time: Displays the MIB node with the longest processing time.

user: Displays SNMP user information.

version: Displays SNMP version.

view: Displays SNMP view information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays SNMP statistics.

```
Hostname> enable
Hostname# show snmp
Chassis: 60FF60
0 SNMP packets input
       0 Bad SNMP version errors
       0 Unknown community name
       0 Illegal operation for community name supplied
       0 Encoding errors
       0 Number of requested variables
       0 Number of altered variables
       0 Get-request PDUs
       0 Get-next PDUs
```

```
       0 Set-request PDUs
0 SNMP packets output
       0 Too big errors (Maximum packet size 1472)
       0 No such name errors
       0 Bad values errors
       0 General errors
       0 Response PDUs
       0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
```

Table 1-1 Output Fields of the show snmp Command

Field	Description
Chassis	System serial number
SNMP packets input	Total number of input packets
Bad SNMP version errors	Total number of packets with version error
Unknown community name	Total number of packets in which an unknown community name is used for access
Illegal operation for community name supplied	Total number of packets in which the community name is used for override operations
Encoding errors	Total number of packets with encoding error
Number of requested variables	Total number of read MIB objects
Number of altered variables	Total number of set MIB objects
Get-request PDUs	Total number of Get request packets
Get-next PDUs	Total number of Get-next request packets
Set-request PDUs	Total number of Set request packets
SNMP packets output	Total number of output packets
Too big errors (Maximum packet size 1472)	Total number of excessively long packets (more than 1,472 bytes)
No such name errors	Total number of packets that contains the no such name error
Bad values errors	Total number of packets that contains the bad values error
General errors	Total number of packets that contains the general error
Response PDU	Total number of packets that are normally returned
Trap PDUs	Total number of sent Trap packets

Field	Description
SNMP global trap	Global Trap enabling/disabling status
SNMP logging	Global SNMP log enabling/disabling status
SNMP agent	Global SNMP agent enabling/disabling status

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 snmp trap link-status

Function

Run the **snmp trap link-status** command to send a Link Trap message through an interface.

Run the **no** form of this command to disable this function.

The Link Trap message sending function is enabled on an interface by default.

Syntax

snmp trap link-status

no snmp trap link-status

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is run, the SNMP sends a Link Trap message if the link status on the interfaces (Ethernet interface, AP interface, and SVI interface) changes. Otherwise, the SNMP does not send the message.

Examples

The following example disables the Link Trap sending function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 snmp-server authentication attempt

Function

Run the **snmp-server authentication attempt** command to configure the maximum number of consecutive SNMP authentication failures and specify the corresponding processing actions.

Run the **no** form of this command to remove this configuration.

The SNMP attack prevention and detection function is disabled by default.

Syntax

snmp-server authentication attempt *attempt-times* **exceed** { **lock** | **lock-time** *lock-time* | **unlock** }

no snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *lock-time* | **unlock** }

Parameter Description

attempt-times: Maximum number of SNMP authentication failures. The value range is from 1 to 10.

exceed: Specifies the actions taken after the SNMP authentication failures exceed the threshold.

lock: Permanently forbids this source IP address from authentication. After this source IP address is placed on the blacklist, the administrator needs to manually unlock the IP address.

lock-time *lock time*: Specifies the lock time of a source IP address after this source IP address is forbidden from authentication, in minutes. The value range is from 1 to 65535.

unlock: Allows a user to log in though the user fails the authentication.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After a source IP address fails the SNMP authentication, the system adds the source IP address to the blacklist. When the number of consecutive authentication failures exceeds the limit, the system restricts subsequent access authentication of this source IP address based on the configured processing actions.

- The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses.
- The source IP addresses that are forbidden in a period of time can be authenticated again after the period expires or after the administrator manually unlocks the IP addresses.
- Unrestricted source IP addresses can be authenticated again based on the correct community name (for SNMPv1 and SNMPv2c) or username (for SNMPv3) so long as users access authentication again.

Examples

The following example sets the consecutive authentication failures of SNMP to 4 and IP address lock time to 30 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Notifications

After the SNMP attack prevention and detection function is enabled, if a source IP address is locked because an incorrect community name or username is used for access authentication, the following notification will be displayed.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 snmp-server chassis-id

Function

Run the **snmp-server chassis-id** command to configure a system serial number.

Run the **no** form of this command to restore the default configuration.

The default system serial number is **60FF60**.

Syntax

snmp-server chassis-id *chassis-id-text*

no snmp-server chassis-id

Parameter Description

chassis-id-text: Text of the system serial number, which may be digits or characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In general, the device serial number is used as the SNMP serial number to facilitate identification of the device. The system sequence number can be displayed by running the **show snmp** command.

Examples

The following example sets the system serial number of SNMP to 123456.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server chassis-id 123456
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 snmp-server community

Function

Run the **snmp-server community** command to configure an authentication name and access permission.

Run the **no** form of this command to remove this configuration.

The default access permission of all communities is read-only.

Syntax

snmp-server community [**0** | **7** | **secret** [**0** | **8**]] *community-string* [**view** *view-name*] [**ro** | **rw**] [**host** *ipv4-address* | **host** *ipv6-address*] [**ipv6** *ipv6-acl-name*] [*acl-name* | *acl-number*]

no snmp-server community [**0** | **7** | **secret** [**0** | **8**]] *community-string*

Parameter Description

0: Indicates that the input community string is a plaintext string.

7: Indicates that the input community string is a ciphertext string.

secret [**0** | **8**]: Indicates that the input community string is encrypted. **0** indicates that the input community string is a plaintext string and is encrypted with the default algorithm. **8** indicates that the input community string is a ciphertext string and is encrypted with the SHA256 algorithm. The default encryption algorithm is SHA256.

community-string: Community string. This parameter is case sensitive and does not support special characters or Chinese characters. The maximum length is 32. It is equivalent to the communication password used between the NMS and SNMP agent.

view *view-name*: Specifies a view name for view-based management.

ro: Specifies that the NMS can only read variables of the MIB.

rw: Specifies that the NMS can read and write variables of the MIB.

host *ipv4-address*: Configures IPv4 host address of SNMP.

host *ipv6-address*: Configures IPv6 host address of SNMP.

ipv6 *ipv6-acl-name*: Specifies the name of a list of IPv6 addresses and the range of the addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to enable the SNMP agent function. It specifies community attributes and NMS scope that is allowed to access the MIB.
- Run the **no snmp-server** command to disable the SNMP agent function.

Examples

The following example allows the NMS to access the MIB with the read-only permission using the SNMP community string named public1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server community public1 ro
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 snmp-server contact

Function

Run the **snmp-server contact** command to configure a system contact mode.

Run the **no** form of this command to remove this configuration.

The contact mode of the system is empty by default.

Syntax

snmp-server contact *contact-text*

no snmp-server contact

Parameter Description

contact-text: String that describes the system contact mode. This parameter is case sensitive and does not support Chinese characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the system contact mode to i-net800@i-net.com.cn.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server contact i-net800@i-net.com.cn
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 snmp-server enable secret-dictionary-check

Function

Run the **snmp-server enable secret-dictionary-check** command to configure password dictionary check for communities and users.

Run the **no** form of this command to remove this configuration.

No password dictionary check is configured for communities and users by default.

Syntax

snmp-server enable secret-dictionary-check

no snmp-server enable secret-dictionary-check

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command must be used with the **password policy** command in global configuration mode.

Examples

The following example sets the password length to be no less than six characters and configures password dictionary check for communities.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy min-size 6
Hostname(config)# snmp-server enable secret-dictionary-check
Hostname(config)# snmp-server community abc12
% The community(abc12) is a weak community!
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **password policy min-size** (security/PASSWORD-POLICY)

1.10 snmp-server enable traps

Function

Run the **snmp-server enable traps** command to enable the agent to actively send Trap messages to the NMS.

Run the **no** form of this command to disable this function.

The SNMP agent is forbidden to send Trap messages to the NMS by default.

Syntax

snmp-server enable traps [*notification-type*]

no snmp-server enable traps

Parameter Description

notification-type: Type of Trap messages that are actively sent. The following types of Trap messages are supported:

authentication: Enables Trap notification for authentication events.

bgp: Enables Trap notification for Border Gateway Protocol (BGP) events.

bridge: Enables Trap notification for bridge events.

entity: Enables Trap notification for entity events.

isis: Enables Trap notification for intermediate system to intermediate system (ISIS) events.

mac-notification: Enables Trap notification for MAC events.

nfpp: Enables Trap notification for Network Foundation Protection Policy (NFPP) events.

ospf: Enables Trap notification for Open Shortest Path First (OSPF) events.

snmp: Enables Trap notification for SNMP events.

urpf: Enables Trap notification for unicast reverse path forwarding (URPF) events.

vrrp: Enables Trap notification for Virtual Router Redundancy Protocol (VRRP) events.

web-auth: Enables Trap notification for Web authentication events.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command must be used with the **snmp-server host** command so that Trap messages can be sent.

- If no Trap type is specified, all types of Trap messages are sent.

Examples

The following example configures the function of actively sending Trap messages for SNMP events.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable traps snmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **snmp-server host**

1.11 snmp-server enable version

Function

Run the **snmp-server enable version** command to configure an SNMP version.

Run the **no** form of this command to disable this version.

All SNMP versions are enabled by default.

Syntax

snmp-server enable version { **v1** | **v2c** | **v3** }

no snmp-server enable version { **v1** | **v2c** | **v3** }

Parameter Description

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the SNMPv1 function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable version v1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 snmp-server flow-control pps

Function

Run the **snmp-server flow-control pps** command to configure SNMP traffic control.

Run the **no** form of this command to restore the default configuration.

About 300 SNMP request packets are processed every second by default.

Syntax

snmp-server flow-control pps *packet-count*

no snmp-server flow-control pps

Parameter Description

packet-count: Number of SNMP request packets processed per second. The value range is from 50 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of SNMP request packets processed per second to 200.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# snmp-server flow-control pps 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 snmp-server group

Function

Run the **snmp-server group** command to configure an SNMP user group.

Run the **no** form of this command to remove this configuration.

No user group is configured by default.

Syntax

snmp-server group *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

no snmp-server group *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

Parameter Description

group-name: Name of a user group.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

auth | **noauth** | **priv**: Configures the security level of SNMPv3 users. **auth** indicates that the messages transmitted by users in this group need authentication but the data does not need encryption. **noauth** indicates that the messages transmitted by users in this group do not need authentication and the data does not need encryption. This security level is valid for SNMPv3 only. **priv** indicates that the messages transmitted by users in this group need authentication and the data needs encryption. This security level is valid for SNMPv3 only.

read *readview*: Associates a read-only view.

write *writeview*: Associates a read/write view.

ipv6 *ipv6-acl-name*: Specifies the name of a list of IPv6 addresses and the range of the addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a user group with the name mib2user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server group mib2user v3 priv read mib2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 snmp-server host

Function

Run the **snmp-server host** command to configure NMS host addresses for the agent to send messages.

Run the **no** form of this command to remove this configuration.

No SNMP host address is configured by default.

Syntax

snmp-server host [**oob**] { *ipv4-addrress* | **ipv6** *ipv6-address*

| **domain** *domain-name*

} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-number*] [**via** *mgmt-name*] [*notification-type*]

no snmp-server host [**oob**] { *ipv4-address* | **ipv6** *ipv6-address*

| **domain** *domain-name*

} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-numer*] [**via** *mgmt-name*]

Parameter Description

oob: Specifies out-of-band communication for the alarm server (sending logs to the alarm server through the management interface).

ipv4-address: IPv4 address of the SNMP host.

ipv6 *ipv6-address*: Specifies the IPv6 address of the SNMP host.

domain *domain-name*: Domain name of the SNMP host.

vrf *vrf-name*: Configures the name of the VRF forwarding table.

informs: Configures the host to send Inform messages.

traps: Configures the host to send Trap messages.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

0: Indicates that the input community string is a plaintext string.

7: Indicates that the input community string is a ciphertext string.

community: Community string.

v3: Uses SNMPv3.

auth | **noauth** | **priv**: Configures the security level of SNMPv3 users. **auth** indicates that the messages transmitted by users in this group need authentication but the data does not need encryption. **noauth** indicates that the messages transmitted by users in this group do not need authentication and the data does not need encryption. This security level is valid for SNMPv3 only. **priv** indicates that the messages transmitted by users in this group need authentication and the data needs encryption. This security level is valid for SNMPv3 only.

username: Username used in SNMPv3 configuration.

udp-port *port-number*: Configures the port ID of the SNMP host. The value range is from 0 to 65535.

via *mgmt-name*: Specifies a management port when OOB is configured. *mgmt-name* indicates the name of the management port.

notification-type: Type of Trap packets, for example, SNMP.

Note

Parameter **0** is not supported if SNMPv3 is used.

Parameter **7** is not supported if SNMPv3 is used.

If no Trap type is specified for the *notification-type* parameter, all types of Trap messages are sent.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used with the **snmp-server enable traps** command to actively send Trap messages to the NMS.
- Multiple SNMP hosts can be configured to receive Trap messages. A host can combine different types of Trap messages, ports, and VRF forwarding tables. If a host is configured with the same port and VRF in multiple configurations, the last configuration is combined with the previous configurations. To send different Trap messages to the same host, configure different types of Trap messages each time. These configurations are finally combined.
- Note: The **via** parameter can be specified only when **oob** is enabled in the command. In this case, the VRF parameter is unavailable.

Examples

The following example sets the SNMP host address to 192.168.12.219 and the community name to public1 and receives Trap messages for SNMP events.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server host 192.168.12.219 public1 snmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **snmp-server enable traps**

1.15 snmp-server inform

Function

Run the **snmp-server inform** command to configure Inform message sending attempts and timeout time.

Run the **no** form Inform this command to restore the default configuration.

The number of default Inform message sending attempts is **3** and the default Inform message timeout time is **15** seconds.

Syntax

snmp-server inform { **retries** *retry-number* | **timeout** *timeout* }

no snmp-server inform

Parameter Description

retries *retry-number*: Specifies the number of Inform message sending attempts. The value range is from 0 to 255.

timeout *timeout*: Specifies the Inform message timeout time, in seconds. The value range is from 0 to 21474836.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of Inform message sending attempts to 5 and Inform message timeout time to 20 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server inform retries 5
Hostname(config)# snmp-server inform timeout 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 snmp-server location

Function

Run the **snmp-server location** command to configure a system location.

Run the **no** form of this command to remove this configuration.

The system location is empty by default.

Syntax

snmp-server location *location-text*

no snmp-server location

Parameter Description

location-text: String that describes the system information. This parameter is case sensitive and does not support Chinese characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the system location as snmp-server location start-technology-city 4F of A Building.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server location start-technology-city 4F of A Building
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 snmp-server logging

Function

Run the **snmp-server logging** command to enable the SNMP logging function.

Run the **no** form of this command to disable this function.

By default, the SNMP logging function is disabled.

Syntax

snmp-server logging { **get-operation** | **set-operation** | **trap-info** }

no snmp-server logging { **get-operation** | **set-operation** | **trap-info** }

Parameter Description

get-operation: Enables the Get and Get-Next operation logging function.

set-operation: Enables the Set operation logging function.

trap-info: Enables the Trap message logging function

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After this command is run, the NMS Get, Get-Next, and Set operations on the SNMP agent are logged. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value.
- Normally, you are advised to disable the SNMP logging function to avoid large amount of logs from affecting device performance.

Examples

The following example enables the Get operation logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server logging get-operation
```

The following example performs Get, Get-Next, and Set operations on the sysname node (.1.3.6.1.2.1.1.5.0) through the NMS and prints the following log information on the console:

```
Hostname#*Feb  7 15:31:16: %SNMP-GET_OPER: NMS source-ip(13.12.11.7) operation(GET)
object(id=1.3.6.1.2.1.1.5.0)
Hostname#*Feb  7 15:32:16:%SNMP-GETN_OPER: NMS source-ip(13.12.11.7)
operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0)
Hostname#*Feb  7 15:33:23: %SNMP-SET_OPER: NMS source-ip(13.12.11.7) operation(SET)
object(id=1.3.6.1.2.1.1.5.0, value=Hostname)
```

The following example disables the Get and Set operation logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no snmp-server logging get-operation
Hostname(config)# no snmp-server logging set-operation
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 snmp-server net-id

Function

Run the **snmp-server net-id** command to configure NE code information of a device.

Run the **no** form of this command to remove this configuration.

The NE code information of a device is empty by default.

Syntax

snmp-server net-id *net-id-text*

no snmp-server net-id

Parameter Description

net-id-text: NE code text of a device. The text is a case-sensitive string of 1 to 255 characters. Space is supported.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the NE code of the device as FZ_CDMA_MSC1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server net-id FZ_CDMA_MSC1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 snmp-server packetsize

Function

Run the **snmp-server packetsize** command to configure the maximum packet length of the SNMP agent.

Run the **no** form of this command to restore the default configuration.

The maximum packet length of the SNMP agent is 1,472 bytes by default.

Syntax

snmp-server packetsize *packetsize*

no snmp-server packetsize

Parameter Description

packetsize: Packet size, in bytes. The value range is from 484 to 17876.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum SNMP packet size to 1,492 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server packetsize 1492
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 snmp-server queue-length

Function

Run the **snmp-server queue-length** command to configure the queue of the Trap messages.

Run the **no** form of this command to restore the default configuration.

The default queue length of the Trap messages is **100**.

Syntax

snmp-server queue-length *queue-length*

no snmp-server queue-length

Parameter Description

queue-length: Queue length. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Adjust the size of the message queue to control the message sending speed.

Examples

The following example sets the queue length of Trap messages to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server queue-length 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 snmp-server source-interface

Function

Run the **snmp-server source-interface** command to configure the source port of a device to receive SNMP packets.

Run the **no** form of this command to restore the default configuration.

The source port of a device with a valid IP address is used to receive SNMP packets by default.

Syntax

snmp-server source-interface *interface-type interface-number*

no snmp-server source-interface

Parameter Description

interface-type interface-number: Interface type and interface number of the source port of a device that receives SNMP packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the source port of a device to receive SNMP packets as Mgmt 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server source-interface Mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 snmp-server system-shutdown

Function

Run the **snmp-server system-shutdown** command to enable the SNMP system reboot notification function.

Run the **no** form of this command to disable this function.

The SNMP system reboot notification function is disabled by default.

Syntax

snmp-server system-shutdown

no snmp-server system-shutdown

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable the SNMP system reboot notification function. The system sends Trap messages to the NMS to notify system reboot before reboot of the device.

Examples

The following example enables the SNMP system reboot notification function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server system-shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 snmp-server trap-format private

Function

Run the **snmp-server trap-format private** command to include private fields in SNMP Trap messages.

Run the **no** form of this command to restore the default configuration.

SNMP Trap messages do not include private fields by default.

Syntax

snmp-server trap-format private

no snmp-server trap-format private

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to include private fields in Trap messages. The supported private field is the alarm generation time. For the specific data types and data ranges of the fields, see the RUIJIE-TRAP-FORMAT-MIB.mib file.
- When SNMPv1 is used to send Trap messages, this configuration does not take effect.

Examples

The following example includes private fields in SNMP Trap messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-format private
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 snmp-server trap-source

Function

Run the **snmp-server trap-source** command to configure a source address for sending Trap messages.

Run the **no** form of this command to restore the default configuration.

The IP address of the interface that sends SNMP packets is used as the source address by default.

Syntax

snmp-server trap-source *interface-type interface-number*

no snmp-server trap-source

Parameter Description

interface-type interface-number: Interface type and interface number of the source port of a device that sends Trap messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the IP address of an interface that sends SNMP packets is used as the source address of the SNMP packets. To manage and identify the source address, you can run this command to configure a fixed local IP address as the source address of the SNMP packets.

Examples

The following example configures the IP address of GigabitEthernet 0/1 as the source address of Trap messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-source gigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 snmp-server trap-timeout

Function

Run the **snmp-server trap-timeout** command to configure the timeout time of Trap message re-sending.

Run the **no** form of this command to restore the default configuration.

The Trap messages are resent with a timeout time of 300 milliseconds by default.

Syntax

snmp-server trap-timeout *trap-timeout-time*

no snmp-server trap-timeout

Parameter Description

trap timeout-time: Timeout time of Trap message re-sending, in 10 milliseconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the timeout time of Trap message re-sending to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-timeout 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 snmp-server udp-port

Function

Run the **snmp-server udp-port** command to configure the ID of a port that receives SNMP packets.

Run the **no** form of this command to restore the default configuration.

The default UDP port ID of the SNMP service is **161**.

Syntax

snmp-server udp-port *port-number*

no snmp-server udp-port

Parameter Description

port-number: ID of a port that receives SNMP packets. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the ID of the UDP port that receives SNMP packets to 15000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server udp-port 15000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 snmp-server user

Function

Run the **snmp-server user** command to configure an SNMP user.

Run the **no** form of this command to remove this configuration.

No SNMP user is configured by default.

Syntax

snmp-server user *username group-name* { **v1** | **v2c** | **v3** [**encrypted** | **interactive**] [**auth** { **md5** | **sha** | **sha2-256** | **sha2-512** } *auth-password*] [**priv** { **des56 | acs128** } *priv-password*] } [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

no snmp-server user *username group-name* { **v1** | **v2c** | **v3** }

Parameter Description

username: Username.

group-name: Name of the user group to which this user belongs.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

encrypted: Ciphertext input as the password input mode. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 authentication key consists of 16 bytes and an SHA authentication key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only.

interactive: Uses the interactive method to configure the authentication and encrypted password string.

auth { **md5** | **sha** | **sha2-256** | **sha2-512** } *auth-password*: Specifies a protocol used for user authentication when an SNMPv3 user is configured.

md5 indicates that MD5 is used for authentication, **sha** indicates that SHA is used for authentication, **sha2-256** indicates that 256-bit SHA2 is used for authentication, **sha2-512** indicates that 512-bit SHA2 is used for authentication, and *auth-password* indicates a password string that is used for authentication protocol configuration. The value range is from 1 to 32 characters. The system converts the passwords into the corresponding authentication keys.

priv { **des56 | acs128** } *priv-password*: Specifies an encryption protocol when an SNMPv3 user is configured.

des56 indicates that 56-bit DES encryption protocol is used, **acs128** indicates that 128-bit ACS encryption protocol is used, and *priv-password* indicates a password string used for encryption. The value is a string of 1 to 32 characters. The system converts the password into the corresponding encryption key.

ipv6 *ipv6-acl-name*: Associates a specified list of IPv6 addresses and specifies the range of the IPv6 NMS addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates an SNMPv3 user user-2 and configures MD5 as an authentication protocol and DES as an encryption protocol.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56
despassstr
```

The following example creates an SNMPv3 user in interaction mode and configures MD5 as an authentication protocol DES and DES as an encryption protocol.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# snmp-server user mib2user mib2group v3 interactive auth md5 priv
des56
Please configure the authentication password (1-32)
Enter Password:************
Confirm Password:************

Please configure the privacy password (1-32)
Enter Password:**********
Confirm Password:**********
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 snmp-server view

Function

Run the **snmp-server view** command to configure an SNMP view.

Run the **no** form of this command to remove this configuration.

The default view allows access to all MIB objects.

Syntax

snmp-server view *view-name oid-tree* { **exclude** | **include** }

no snmp-server view *view-name* [*oid-tree*]

Parameter Description

view-name: View name.

oid-tree: MIB objects associated with a view, which are displayed as an MIB subtree.

exclude: Indicates that the MIB object subtree is not included in the view.

include: Indicates that the MIB object subtree is included in the view.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a view named mib2 and includes all MIB-2 subtrees with OID 1.3.6.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server view mib2 1.3.6.1 include
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 RMON Commands

Command	Function
rmon alarm	Configure the Remote Network Monitoring (RMON) alarm function.
rmon collection history	Configure the history statistics function on an Ethernet interface.
rmon collection stats	Configure the statistics function on an Ethernet interface.
rmon event	Configure an RMON event.
show rmon	Display all RMON information.
show rmon alarm	Display the alarm table information.
show rmon event	Display the event table information.
show rmon history	Display the history table information.
show rmon statistics	Display the Ethernet statistics information.

1.1 rmon alarm

Function

Run the **rmon alarm** command to configure the Remote Network Monitoring (RMON) alarm function.

Run the **no** form of this command to remove this configuration.

The RMON alarm function is not configured by default.

Syntax

rmon alarm *alarm-table-index alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *ampling-rising-threshold-value* [*event-number*] **falling-threshold** *falling-threshold-value* [*event-number*] [**owner** *owner-name*]

no rmon alarm *alarm-table-index*

Parameter Description

alarm-table-index: Index number of an alarm table. The value range is from 1 to 65535.

alarm-variable: Alarm variable. The value is a string of 1 to 255 characters and is represented in the format of entry.integer.instance, for example, 1.3.6.1.2.1.2.1.10.1.

sampling-interval: Collection interval, in seconds. The value range is from 1 to 2147483647.

absolute | **delta**: Configures a collection type. **absolute** indicates absolute value sampling. That is, variable values are extracted directly when sampling starts. **delta** indicates changing value sampling. That is, changing values are extracted in the sampling interval when sampling starts.

rising-threshold *sampling-rising-threshold-value*: Configures an upper limit of sampled objects. The value range is from -2147483648 to 2147483647.

event-number: Index number of an event whose event number is *event-number* when the upper or lower limit is reached. The value range is from 1 to 65535.

falling-threshold *falling-threshold-value*: Configures a lower limit to sampled objects. The value range is from -2147483648 to 2147483647.

owner *owner-name*: Configures an entry creator. The value is a case-sensitive string of 1 to 63 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to modify parameters of configured alarm entries, including alarm variable, sampling type, entry creator, sampling interval, upper/lower limit, and event.

Examples

The following example monitors the management information base (MIB) variable instance **ifInNUcastPkts.6**, sets the sampling interval to 60 seconds, and triggers event 1 when the variable value reaches the upper limit 20 or lower limit 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 60 delta rising-threshold 20
1 falling-threshold 10 1 owner UserA
```

Notifications

- If the configuration you delete is not configured, the following notification will be displayed.
- If the upper limit is smaller than or equal to the lower limit, the following notification will be displayed.
- If the entered object OID is not improper, the following notification will be displayed.
- If the number of configured entries reaches the upper limit, the following notification will be displayed.
- If a memory application failed, the following notification will be displayed.

Common Errors

- The entered object OID is improper. For example, the variable corresponding to this OID is not configured or the OID type is not an integer or unsigned integer.
- The upper limit is smaller than or equal to the lower limit.

Platform Description

N/A

Related Commands

N/A

1.2 rmon collection history

Function

Run the **rmon collection history** command to configure the history statistics function on an Ethernet interface.

Run the **no** form of this command to remove this configuration.

The history statistics function is not configured on an Ethernet interface by default.

Syntax

rmon collection history *collection-history-table-index* [**buckets** *bucket-number*] [**interval** *period-time*] [**owner** *owner-name*]

no rmon collection history *collection-history-table-index*

Parameter Description

collection-history-table-index: Index number of a history control table. The value range is from 1 to 65535.

owner *owner-name*: Configures an entry creator. The value is a case-sensitive string of 1 to 63 characters.

buckets *bucket-number*: Configures the capacity of a history statistics table. The value range is from 1 to 65535. Actually, only 10 history entries are configured.

interval *period-time*: Configures a collection period, in seconds. The value range is from 1 to 3600, and the default value is **1800**.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- It is not allowed to modify parameters of the configured history control entries.
- It is not allowed to delete history statistics entries configured on another interface on the local interface.

Examples

The following example configures the history statistics function on GigabitEthernet 0/1 and sets the capacity of the history statistics table to 5 and collection period to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-GigabitEthernet0/1)# rmon collection history 1 owner UserA buckets
5 interval 60
```

Notifications

- If the configuration you delete is not configured, the following notification will be displayed.
- If you modify parameters of the configured history control entries, the following notification will be displayed.
- If the number of configured entries reaches the upper limit, the following notification will be displayed.
- If a memory application failed, the following notification will be displayed.

Common Errors

The parameters of configured history control entries are reconfigured or modified.

Platform Description

N/A

Related Commands

N/A

1.3 rmon collection stats

Function

Run the **rmon collection stats** command to configure the statistics function on an Ethernet interface.

Run the **no** form of this command to remove this configuration.

The Ethernet statistics function is not configured on an Ethernet interface by default.

Syntax

rmon collection stats *collection-stats-table-index* [**owner** *owner-name*]

no rmon collection stats *collection-stats-table-index*

Parameter Description

collection-stats-table-index: Index number of a statistics entry. The value range is from 1 to 65535.

owner *owner-name*: Configures an entry creator. The value is a case-sensitive string of 1 to 63 characters. Space is not supported.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

- It is not allowed to modify parameters of configured statistics entries.
- It is not allowed to delete history statistics entries configured on another interface on the local interface.

Examples

The following example configures the statistics function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-GigabitEthernet0/1)# rmon collection stats 1 owner UserA
```

Notifications

- If the configuration you delete is not configured, the following notification will be displayed.
- If you modify parameters of the configured statistics entries, the following notification will be displayed.
- If the number of configured entries reaches the upper limit, the following notification will be displayed.
- If a memory application failed, the following notification will be displayed.

Common Errors

The parameters of configured statistics entries are reconfigured or modified.

Platform Description

N/A

Related Commands

N/A

1.4 rmon event

Function

Run the **rmon event** command to configure an RMON event.

Run the **no** form of this command to remove this configuration.

No RMON event is configured by default.

Syntax

rmon event *event-table-index* [**description** *description-string*] [**log**] [**owner** *owner-name*] [**trap** *community*]

no rmon event *event-table-index*

Parameter Description

event-table-index: Index number of an event table. The value range is from 1 to 65535.

description d*escription-string*: Configures description of an event. The value is a string of 1 to 127 characters.

log: Specifies a log event. When a log event is triggered, the system generates a record in the log. The default number of log records is 10. If a new record is generated, the earliest record is deleted.

owner *owner-name*: Configures an entry creator. The value is a case-sensitive string of 1 to 63 characters.

trap *community*: Specifies a Trap event. When a Trap event is triggered, the system sends a Trap message with the community name *community*.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be used to modify parameters of configured event entries, including event table type, community name, creator, and description.

Examples

The following example defines actions of an event: generating an event record "ifInNUcastPkts is abnormal" and sending a Trap message with the community name being public.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# rmon event 1 log trap public description "ifInNUcastPkts is abnormal"
owner UserA
```

Notifications

- If the configuration you delete is not configured, the following notification will be displayed.
- If the number of configured entries reaches the upper limit, the following notification will be displayed.
- If a memory application failed, the following notification will be displayed.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 show rmon

Function

Run the **show rmon** command to display all RMON information.

Syntax

show rmon

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display all RMON information, including all alarm entries, event entries, event record entries, history control entries, history record entries, and statistics entries.

Examples

The following example displays all RMON information.

```
Hostname> enable
Hostname# show rmon
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1
                owner = admin
                status = 0
                dropEvents = 61
                octets = 170647461
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
                packets128To255Octets = 2098146
                packets256To511Octets = 126716
                packets512To1023Octets = 363621
```

```
                packets1024To1518Octets = 1077865
rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1
                bucketsRequested = 5
                bucketsGranted = 5
                interval = 60
                owner = UserA
                stats = 1
rmon history table:
                index = 1
                sampleIndex = 2485
                intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
……
rmon alarm table:
                index: 1
                interval: 60
                oid = 1.3.6.1.2.1.2.2.1.12.6
                sampleType: 2
                alarmValue: 0
                startupAlarm: 3
                risingThreshold: 20
                fallingThreshold: 10
                risingEventIndex: 1
                fallingEventIndex: 1
                owner: UserA
                status: 1
rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal
                type = 4
                community = public
                lastTimeSent = 0d:0h:0m:0s
                owner =UserA
```

```
                status = 1
rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6 d:19 h:21 m:48 s
                logDescription = ifInNUcastPkts is abnormal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show rmon alarm

Function

Run the **show rmon alarm** command to display the alarm table information.

Syntax

show rmon alarm

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the alarm table information.

```
Hostname> enable
Hostname# show rmon alarm
rmon alarm table:
                index: 1
                interval: 60
```

```
oid = 1.3.6.1.2.1.2.2.1.12.6
sampleType: 2
alarmValue: 0
startupAlarm: 3
risingThreshold: 20
fallingThreshold: 10
risingEventIndex: 1
fallingEventIndex: 1
owner: UserA
status: 1
```

Table 1-1 Output Fields of the show rmon alarm Command

Field	Description
rmon alarm table	Alarm table
index	Index of an alarm table
interval	Sampling comparison interval
oid	Object OID
sampleType	Comparison type: delta or absolute
alarmValue	Object value
startupAlarm	Alarm type, for example, upper limit alarm
risingThreshold	Upper limit
fallingThreshold	Lower limit
risingEventIndex	Index of an event corresponding to the upper limit
fallingEventIndex	Index of an event corresponding to the lower limit
owner	Entry creator
status	Entry state

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show rmon event

Function

Run the **show rmon event** command to display the event table information.

Syntax

show rmon event

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the event table information.

```
Hostname> enable
Hostname# show rmon event
rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal
                type = 4
                community = public
                lastTimeSent = 0d:0h:0m:0s
                owner =UserA
                status = 1
rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6d:19h:21m:48s
                logDescription = ifInNUcastPkts is abnormal
```

Table 1-2 Output Fields of the show rmon event Command

Field	Description
rmon event table	Event table

Field	Description
index	Index of an event table
description	Description of an event table
type	Comparison type: delta or absolute
community	SNMP community name
lastTimeSent	Generation time of the last log message
owner	Entry creator
status	Entry state
rmon log table	Log table
eventIndex	Index of an event table
logTime	Logging time corresponding to an event table
logDescription	Log description

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show rmon history

Function

Run the **show rmon history** command to display the history table information.

Syntax

show rmon history

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the history group information.

```
Hostname> enable
Hostname# show rmon history
rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1
                bucketsRequested = 5
                bucketsGranted = 5
                interval = 60
                owner = UserA
                stats = 1
rmon history table:
                index = 1
                sampleIndex = 2485
                intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

Table 1-3 Output Fields of the show rmon history Command

Field	Description
rmon history control table	History statistics control table
index	Index of a history statistics control table
interface	Interface name
bucketsRequested	Number of requests
bucketsGranted	Capacity of history entries allowed

Field	Description
interval	Sampling interval
owner	Entry creator
stats	Entry state
rmon history table	History statistics table
sampleIndex	Index of a history table
intervalStart	Generation time
dropEvents	Number of received packets that are lost due to insufficient resources
octets	Number of received bytes
pkts	Number of received packets
broadcastPkts	Number of received broadcast packets
multiPkts	Number of received multicast packets
crcAlignErrors	Number of packets with CRC errors
underSizePkts	Number of packets in the correct format and with a length being less than 64 bytes
overSizePkts	Number of packets in the correct format and with a length being more than 1,518 bytes
fragments	Number of packets with a length being less than 64 bytes and with CRC or alignment errors
jabbers	Number of packets with a length being more than 1,518 bytes and with CRC or alignment errors
collisions	Total number of conflicts
utilization	Network utilization

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show rmon statistics

Function

Run the **show rmon statistics** command to display the Ethernet statistics information.

Syntax

show rmon statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the Ethernet statistics information.

```
Hostname> enable
Hostname# show rmon statistics
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1
                owner = admin
                status = 0
                dropEvents = 61
                octets = 170647461
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
                packets128To255Octets = 2098146
```

```
                packets256To511Octets = 126716
                packets512To1023Octets = 363621
                packets1024To1518Octets = 1077865
```

Table 1-4 Output Fields of the show rmon statistics Command

Field	Description
ether statistic table	Ethernet statistics table
Index	Index of an Ethernet statistics table
Interface	Interface name
Owner	Entry creator
Status	Entry state
dropEvents	Number of received packets that are dropped due to insufficient resources
octets	Number of received bytes
pkts	Number of received packets, including error packets, broadcast packets, and multicast packets
broadcastPkts	Number of received broadcast packets
multiPkts	Number of received multicast packets
crcAlignErrors	Number of packets with CRC and frame alignment errors
underSizePkts	Number of received packets in the correct format and with a length being less than 64 bytes
overSizePkts	Number of received packets in the correct format and with a length being more than 1,518 bytes
fragments	Number of received packets with a length being less than 64 bytes and with CRC or frame alignment errors
jabbers	Number of received packets with a length being more than 1,518 bytes and with CRC or frame alignment errors
collisions	Total number of conflicts
packets64Octets	Number of 64-byte packets, including packets with errors
packets65To127Octets	Number of packets with a length from 64 bytes to 127 bytes, including packets with errors
packets128To255Octets	Number of packets with a length from 128 bytes to 255 bytes, including packets with errors
packets256To511Octets	Number of packets with a length from 256 bytes to 511 bytes, including packets with errors

Field	Description
packets512To1023Octets	Number of packets with a length from 512 bytes to 1023 bytes, including packets with errors
packets1024To1518Octets	Number of packets with a length from 1,024 bytes to 1,518 bytes, including packets with errors

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 CWMP Commands

Command	Function
acs password	Configure an ACS password for CWMP connection.
acs url	Configure an ACS URL for CWMP connection.
acs username	Configure an ACS username for CWMP connection.
cpe back-up	Enable the backup and restoration function of the CPE main program or configuration file.
cpe inform	Enable the periodic Inform function of the CPE.
cpe source interface	Obtain an IP address through the specified interface and configure a CPE URL for CWMP connection. based on the IP address.
cpe password	Configure a CPE password for CWMP connection.
cpe url	Configure a CPE URL for CWMP connection.
cpe username	Configure a CPE username for CWMP connection.
cwmp	Enable the CWMP function and enter the CWMP configuration mode.
disable download	Disable the management function of receiving any main program and configuration file delivered by the ACS.
disable upload	Disable the management function of uploading any main program, configuration file and log file to the ACS.
show cwmp configuration	Display the current configuration of the CWMP function.
show cwmp status	Display the current running status of CWMP.
timer cpe-timeout	Configure the CPE timeout time in the case of no ACS response.

1.1 acs password

Function

Run the **acs password** command to configure an ACS password for CWMP connection.

Run the **no** form of this command to remove this configuration.

No ACS password is configured for CWMP connection by default.

Syntax

acs password { **0** *encryption-type* | **7** *encrypted-password* | *password* }

no acs password

Parameter Description

0 *encryption-type*: Specifies a plaintext password as the password encryption type.

7 *encrypted-password*: Specifies a cyphertext string. The cyphertext encrypted using encryption algorithms must be legal, for example, it must be an even number and less than or equal to 256 characters.

password: ACS password for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

When an ACS password is configured for CWMP connection, the encryption type does not need to be entered. If an encrypted password is copied and pasted, the encryption type must be entered. A valid password should meet the following format requirements:

- Contain letters or digits.
- Trailing and middle spaces are a part of the password.

Examples

The following example sets the ACS password for CWMP connection to 123user_1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# acs password 123user_1
```

Notifications

If the entered password is cyphertext and it is not an even number or its length is less than 2 characters or more than 254 characters, the following notification will be displayed:

```
Invalid Encrypted Password
```

If the entered password is plaintext and longer than 126 characters, the following notification will be displayed:

```
The Length of ACS's Password is Too Long
```

If the entered password is plaintext and contains invalid characters, the following notification will be displayed:

```
Password String Include Invalid Characters!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 acs url

Function

Run the **acs url** command to configure an ACS URL for CWMP connection.

Run the **no** form of this command to remove this configuration.

No ACS URL is configured for CWMP connection by default.

Syntax

acs url *url*

no acs url

Parameter Description

url: ACS URL for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

If the ACS URL is not manually configured but a dynamic ACS URL is obtained through DHCP, this dynamic ACS URL is used to initiate a connection to the ACS. Ensure that UDP port 7547 on the CPE is unused. This port is used for Simple Traversal of UDP over NATs (STUN) port listening. The ACS URL must meet the following format requirements:

- Follow the format of http://ip[:port]/path.
- Contain 255 characters at most.

Examples

The following example sets the ACS URL for connection with the CPE to http://10.10.10.1:7547/acs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
```

```
Hostname(config-cwmp)# acs url http://10.10.10.1:7547/acs
```

Notifications

If the ACS URL is null, the following notification will be displayed:

```
input acs attribute parameter is null
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 acs username

Function

Run the **acs username** command to configure an ACS username for CWMP connection.

Run the **no** form of this command to remove this configuration.

No ACS username is configured for CWMP connection by default.

Syntax

acs username *username*

no acs username

Parameter Description

username: ACS username for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example sets the ACS username for CWMP connection to **admin**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# acs username admin
```

Notifications

If the ACS username is null, the following notification will be displayed:

```
input acs attribute parameter is null
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 cpe back-up

Function

Run the **cpe back-up** command to enable the backup and restoration function of the CPE main program or configuration file.

Run the **no** form of this command to disable this function.

The backup and restoration function of the main program or configuration file is disabled by default.

Syntax

cpe back-up [**delay-time** *time*]

no cpe back-up

Parameter Description

time: Delay for backup and restoration of the CPE main program or configuration file, in seconds. The value range is from 30 to 1000, and the default value is **60**.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

After the backup and restoration of the main program or configuration file is enabled on the CPE in the case of an abnormality, the CPE can restore its abnormal main program or configuration file to their previous states in time when the CPE fails to connect to the ACS and breaks away from the management center after the main program or configuration file upgrade. The ACS is restored to manage the CPE. This abnormality is generally caused by delivery of an incorrect main program version or configuration file.

Examples

The following example configures the backup and restoration function of the CPE main program or configuration file.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe back-up
```

Common Errors

N/A

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 cpe inform

Function

Run the **cpe inform** command to enable the periodic Inform function of the CPE.

Run the **no** form of this command to disable this function.

The periodic Inform function of the CPE is disabled by default.

Syntax

cpe inform [**interval** *interval*] [**start-time** *hh:mm:ss MM/DD/YY*]

no cpe inform

Parameter Description

interval *interval*: Configures the periodic Inform interval of the CPE, in seconds. The value range is from 30 to 3600, and the default value is **600**.

start-time *hh:mm:ss MM/DD/YY*: Configures the start time of periodic Inform. *hh* indicates hour. *mm* indicates minute. *ss* indicates second. *MM* indicates month. *DD* indicates day. *YY* indicates year.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

- The shorter the CPE periodic Inform interval is, the more timely the ACS traces the latest status of the CPE. More CPE-ACS sessions consume more resources. Users must configure a proper interval based on the current network status and ACS performance configuration.
- If no Inform start time is configured, from the Inform enabling time, Inform is performed once every default

Inform interval.

- If the Inform start time is configured, periodic Inform starts at the specified start time. For example, if the Inform interval is set to 60 seconds and the start time is 12:00 a.m. next day, periodic Inform will start at 12:00 a.m. next day and be performed once every 60 seconds.

Examples

The following example sets the periodic Inform interval of the CPE to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe inform interval 60
```

Common Errors

N/A

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 cpe source interface

Function

Run the **cpe source interface** command to obtain an IP address through the specified interface and configure a CPE URL for CWMP connection. based on the IP address.

Run the **no** form of this command to remove this configuration.

No IP address is obtained through the specified interface and used to configure a CPE URL for CWMP connection by default.

Syntax

cpe source interface *interface-type interface-number* [**port** *port-number*]

no cpe source interface

Parameter Description

interface-type interface-number: Type and number of the port of CPE URL for CWMP connection.

port *port-number*: Specifies a port number. The value range is from 1 to 65535, and the default value is **7547**.

Command Modes

CWMP configuration mode

Default Level

14

Usage Guidelines

- This command and the **cpe url** command cannot be configured at the same time. If either command is configured, the other command must not be configured or must be deleted. If the two commands are not configured, the CPE automatically selects its URL based on the ACS URL.
- The interface name of the CPE must be the full name of the interface and can be automatically filled when a CLI command is entered.
- If no port ID is configured, the default port ID 7547 is used.

Examples

The following example configures a CPE URL for CWMP connection and sets the CPE port ID to 7547 on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe source interface GigabitEthernet 0/1 port 7547
```

Notifications

If the name of the entered interface is incorrect, the following notification will be displayed:

```
% Invalid input detected at '^' marker.
```

If an IP address is configured using the **cpe url** command, the following notification will be displayed:

```
Cpe url have been set by command cpe url, please clear it.
```

Common Errors

N/A

Platform Description

If this command is configured on the CPE, running the **show cwmp configuration** command displays one more record, which is the full name of the interface. If this command is not configured on the CPE, running the **show cwmp configuration** command displays no information.

```
Hostname> enable
Hostname# show cwmp configuration
CWMP status                 : enable
ACS URL                     : http://118.190.126.198/service/acs/ABC0020176681
ACS username                :
ACS password                :
CPE URL                     : http://192.168.197.106:7547/ (DYNAMIC)
CPE source interface name      : GigabitEthernet 0/1
CPE username                :
CPE password                :
CPE inform status            : enable
CPE inform interval          : 180s
```

```
CPE inform start-time          : 0:0:0 0 0 0
CPE wait timeout              : 30s
CPE download status           : enable
CPE upload status             : enable
CPE back up status            : enable
CPE back up delay time         : 60s
CPE STUN port-adaptive         : disable
CPE STUN port                 : 3478
CPE STUN max-period           : 60s
CPE STUN min-period           : 20s
```

Related Commands

N/A

1.7 cpe password

Function

Run the **cpe password** command to configure a CPE password for CWMP connection.

Run the **no** form of this command to remove this configuration.

No CPE password is configured for CWMP connection by default.

Syntax

cpe password { **0** *encryption-type* | **7** *encrypted-password* | *password* }

no cpe password

Parameter Description

0 *encryption-type*: Specifies a plaintext password as the password encryption type.

7 *encrypted-password*: Specifies a cyphertext string. The cyphertext encrypted using encryption algorithms must be legal, for example, it must be an even number and less than or equal to 256 characters.

password: CPE password for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

When a CPE password is configured for CWMP connection, the encryption type does not need to be entered. If an encrypted password is copied and pasted, the encryption type must be entered. A valid password should meet the following format requirements:

- Contain 1 to 26 characters including uppercase letters, lowercase letters, and digits.
- Leading spaces will be ignored, while the trailing and middle spaces are valid.

Examples

The following example sets the CPE password for CWMP connection to 123user_1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe password 123user_1
```

Notifications

If the entered password is cyphertext and it is not an even number or its length is less than 2 characters or not more than 254 characters, the following notification will be displayed:

```
Invalid Encrypted Password
```

If the entered password is plaintext and longer than 126 characters, the following notification will be displayed:

```
The Length of ACS's Password is Too Long
```

If the entered password is plaintext and contains illegal characters, the following notification will be displayed:

```
Password String Include Invalid Characters!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 cpe url

Function

Run the **CPE url** command to configure a CPE URL for CWMP connection.

Run the **no** form of this command to remove this configuration.

No CPE URL is configured for CWMP connection by default.

Syntax

cpe url *url*

no cpe url

Parameter Description

url: CPE URL for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

If the CPE URL is not manually configured, a CPE URL is automatically selected based on the ACS URL. The CPE URL format must meet the following requirements:

- Follow the http://ip [: port]/ format.
- Contain 255 characters at most.

Examples

The following example sets the CPE URL for CWMP connection to http://10.10.10.1:7547/.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/
```

Notifications

If the CPE URL is null, the following notification will be displayed:

```
input CPE attribute parameter is null
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 cpe username

Function

Run the **cpe username** command to configure a CPE username for CWMP connection.

Run the **no** form of this command to remove this configuration.

No CPE username is configured for CWMP connection by default.

Syntax

cpe username *username*

no cpe username

Parameter Description

username: CPE username for CWMP connection.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example sets the CPE username for CWMP connection to **admin**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# cpe username admin
```

Notifications

If the CPE username is null, the following notification will be displayed:

```
input acs attribute parameter is null
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 cwmp

Function

Run the **cwmp** command to enable the CWMP function and enter the CWMP configuration mode.

Run the **no** form of this command to disable this function.

The CWMP function is disabled by default.

Syntax

cwmp

no cwmp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example enables the CWMP function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 disable download

Function

Run the **disable download** command to disable the management function of receiving any main program and configuration file delivered by the ACS.

Run the **no** form of this command to remove this configuration.

The management function of receiving any main program and configuration file delivered by the ACS is enabled by default.

Syntax

disable download

no disable download

Parameter Description

N/A

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.

Examples

The following example disables the management function of receiving any main program and configuration file delivered by the ACS.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# disable download
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 disable upload

Function

Run the **disable upload** command to disable the management function of uploading any main program, configuration file and log file to the ACS.

Run the **no** form of this command to remove this configuration.

The management function of uploading any main program, configuration file and log file to the ACS is enabled by default.

Syntax

disable upload

no disable upload

Parameter Description

N/A

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example disables the management function of uploading any main program, configuration file and log file to the ACS.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# disable upload
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show cwmp configuration

Function

Run the **show cwmp configuration** command to display the current configuration of the CWMP function.

Syntax

show cwmp configuration

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the current configuration of the CWMP function.

```
Hostname> enable
```

```
Hostname# show cwmp configuration
CWMP Status                  : enable
ACS URL                     : http://www.Hostname.com.cn/acs
ACS username                 : admin
ACS password                 : ******
CPE source interface name      :
CPE URL                     : http://10.10.10.2:7547/
CPE username                 : Hostname
CPE password                 : ******
CPE inform status             : disable
CPE inform interval           : 60s
CPE inform start time         : 0:0:0 0 0 0
CPE wait timeout             : 50s
CPE download status           : enable
CPE upload status            : enable
CPE back up status            : enable
CPE back up delay time         : 60s
CPE STUN port-adaptive         : disable
CPE STUN probe nat agingtime    : disable
CPE STUN port                : 3478
CPE STUN max-period           : 60s
CPE STUN min-period           : 20s
```

Table 1-1 Output Fields of the show cwmp configuration Command

Field	Description
CWMP Status	Enabling status of the CWMP function
ACS URL	ACS URL for CWMP connection
ACS username	ACS username for CWMP connection
ACS password	ACS password for CWMP connection
CPE source interface name	CPE URL port for CWMP connection
CPE URL	CPE URL for CWMP connection
CPE username	CPE username for CWMP connection
CPE password	CPE password for CWMP connection
CPE inform status	Periodic Inform status of CPE
CPE inform interval	Periodic Inform interval of CPE
CPE wait timeout	CPE session timeout time
CPE inform start time	Start time of periodic Inform of CPE
CPE download status	Whether to download any main program and configuration file from the ACS

Field	Description
CPE upload status	Whether to upload any main program and configuration file and log file to the ACS
CPE back up status	Whether to enable restoration of the main program and configuration file
CPE back up delay time	Delay for restoration of the main program and configuration file
CPE STUN port-adaptive	Whether to enable STUN port auto-adaption: ● **disable**: Disables the STUN port auto-adaption function. ● **enable**: Enables the STUN port auto-adaption function.
CPE STUN probe nat agingtime	Whether to enable the STUN NAT age time probe function: ● **disable**: Disables the STUN NAT age time probe function. ● **enable**: Enables the STUN NAT age time probe function.
CPE STUN port	STUN server port
CPE STUN max-period	Maximum keep-alive time of STUN packets
CPE STUN min-period	Minimum keep-alive time of STUN packets

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 show cwmp status

Function

Run the **show cwmp status** command to display the current running status of CWMP.

Syntax

show cwmp status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the current running status of CWMP.

```
Hostname> enable
Hostname# show cwmp status
CWMP Status                  : enable
Session status               : Close
Last success session         : Unknown
Last success session time    : Thu Jan  1 00:00:00 1970
Last fail session            : Unknown
Last fail session time       : Thu Jan  1 00:00:00 1970
Session retry times          : 0
```

Table 1-2 Output Fields of the show cwmp status Command

Field	Description
CWMP Status	Enabling status of the CWMP function
Session status	Status of the current session between the CPE and ACS
Last success session	Type of the last successful session
Last success session time	End time of the last successful session
Last fail session	Type of the last failed session
Last fail session time	End time of the last failed session
Session retry times	Retry times of the current session

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 timer cpe-timeout

Function

Run the **timer cpe-timeout** command to configure the CPE timeout time in the case of no ACS response.

Run the **no** form of this command to remove this configuration.

The default CPE timeout time is **30** seconds in the case of no ACS response.

Syntax

timer cpe-timeout *tiemout*

no timer cpe-timeout

Parameter Description

timeout: Timeout time, in seconds. The value range is from 10 to 600.

Command Modes

CWMP configuration mode

Default Level

1

Usage Guidelines

This command is used to configure the CPE timeout time in the case of no ACS response. This CPE timeout time refers to the maximum delay of a session when the CPE fails to receive ACS response due to an exception, for example, network disconnection.

Examples

The following example sets the CPE timeout time to 50 seconds in the case of no ACS response.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# timer cpe-timeout 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 SEM Commands

Command	Function
action cli	Configure a policy by running a specified command line.
action counter	Configure an action for a policy by operating a specified SEM naming counter.
action exit	Configure an action for a policy by terminating a policy script and exiting the current status.
action reload	Configure an action for a policy by restarting a device.
action set	Configure an action for a policy by setting local variables.
action syslog	Configure an action of logging.
action wait	Configure an action for a policy by pausing a policy script.
commit	Submit policy configuration.
description	Configure the description of an SEM policy.
event tag counter	Configure a counter monitoring event.
event tag interface	Configure an interface monitoring event.
event tag syslog	Configure a log monitoring event.
event tag timer	Configure a timer monitoring event.
event tag track	Configure a track monitoring event.
list-config	Display the current policy configuration.
policy record	Enable the function of recording CLI command output and configure output size.
rollback	Roll back the current policy configuration.
show smart manager detector	Display detector information.

show smart manager history events	Display event history information.
show smart manager policy all	Display all policies and their submission information.
show smart manager policy registered	Display registered policies.
show smart manager version	Display SEM versions.
smart manager applet	Create an SEM policy.
smart manager detector event-number	Configure upper limits of SEM detector parameters.
smart manager global-variant number	Configure the maximum number of global variables of SEM.
smart manager policy	Configure upper limits of SEM policy parameters.
smart manager record	Configure upper limits of SEM policy instance parameters.
smart manager schdulr	Configure upper limits of SEM policy scheduler parameters.

1.1 action cli

Function

Run the **action cli** command to configure a policy by running a specified command line.

Run the **no** form of this command to remove this configuration.

No action is configured for a policy by default.

Syntax

action *action-label* **cli command** *cli-string* [**pattern** *pattern-string*]

no action *action-label*

Parameter Description

action-label: Label of an action.

command *cli-string*: Specifies the command content to be run.

pattern *pattern-string*: Specifies the interaction reply content of a command.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- The *pattern-string* parameter separates multiple interaction replies with space. If a reply contains space, the double quotes ("") are used for discrimination.
- Command output of a policy can be recorded to the file system of a device. The **policy record** command is run to enable the recording function and configure file size, and the **smart manager policy record clean** command is run to clear command output records. For more information, see **policy record**.

Examples

The following example runs the **enable**, **clear arp-cache**, and **clear ip route *** commands for the none events in the clear_cache policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet clear_cache
Hostname(config-applet)# event tag monitor_cmd none
Hostname(config-applet)# action 00 cli command "enable"
Hostname(config-applet)# action 10 cli command "clear arp-cache"
Hostname(config-applet)# action 20 cli command "clear ip route *"
```

```
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **policy record**
- **smart manager applet**

1.2 action counter

Function

Run the **action counter** command to configure an action for a policy by operating a specified SEM naming counter.

Run the **no** form of this command to remove this configuration.

No action is configured for a policy by default.

Syntax

action *action-label* **counter name** *counter-name* **value** *counter-value* **op** { **dec** | **inc** | **nop** | **set** }

no action *action-label*

Parameter Description

action-label: Label of an action.

name *counter-name*: Specifies the name of a counter to be operated.

value *counter-value*: Specifies a value used by an operation. The value range is from -2147483648 to 2147483647.

op { **dec** | **inc** | **nop** | **set** }: Specifies a method used by an operation. **dec** indicates a decrement of the counter value based on the value of **value** *counter-value*. **inc** indicates an increment of the counter value based on the value of **value** *counter-value*. **nop** indicates the reading of the counter value, and **set** specifies the counter value.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a log monitoring policy Test_1 and sets the action of the policy to increase the value of the Authenticate_Faile counter by 1 when the content "login faile" is detected in the log.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_log syslog pattern "login faile"
Hostname(config-applet)# action 00 counter name Authenticate_Faile op inc
value 1
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.3 action exit

Function

Run the **action exit** command to configure an action for a policy by terminating a policy script and exiting the current status.

Run the **no** form of this command to remove this configuration.

The value **1** is returned by default when a policy is run to the end.

Syntax

action *action-label* **exit** [*result*]

no action *action-label*

Parameter Description

action-label: Label of an action.

result: Returned value of **exit**. The value range is from 0 to 2147483647. The default value is **1**.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

In the synchronous mode, the operation that triggers a policy will wait for the policy to complete and determine whether to continue running the policy based on the returned value of the policy. If the returned value is 0, the policy stops running. If the returned value is another value, the policy continues running.

Examples

The following example configures a policy Test_1 to monitor the command lines in the synchronous mode and forbids user operation and displays a notification when the user enters "write memory".

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_cli cli pattern "write memory"
sync yes
Hostname(config-applet)# action 00 puts "can not do this"
Hostname(config-applet)# action 10 exit 0
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Related Commands

- **smart manager applet**

1.4 action reload

Function

Run the **action reload** command to configure an action for a policy by restarting a device.

Run the **no** form of this command to remove this configuration.

No action is configured for a policy by default.

Syntax

action *action-label* **reload**

no action *action-label*

Parameter Description

action-label: Label of an action.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a policy Test_1 to restart a device when the total memory of the device is less than 20 MB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_memory sysmon memory scope
system-free entry-op lt entry-val 20000
Hostname(config-applet)# action 00 reload
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.5 action set

Function

Run the **action set** command to configure an action for a policy by setting local variables.

Run the **no** form of this command to remove this configuration.

No local variable of SEM is configured by default.

Syntax

action *action-label* **set** *variable-name variable-value*

no action *action-label*

Parameter Description

action-label: Label of an action.

variable-name: Name of a local variable.

variable-value: Value of a local variable.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

A configured local variable can have the same name as a global variable. If the configured local variable has the same name as a global variable, the local variable takes priority over the global variable when this variable name is used to visit a variable.

Examples

The following example configures a policy Test_1, sets variables in the policy of the none event type, and sends the variables to a log.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag none_event none
Hostname(config-applet)# action 00 set var_for_test "Test_1 running"
Hostname(config-applet)# action 10 syslog msg "$var_for_test"
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.6 action syslog

Function

Run the **action syslog** command to configure an action of logging.

Run the **no** form of this command to remove this configuration.

No action is configured for a policy by default.

Syntax

action *action-label* **syslog** [**facility** *mnemonics*] **msg** *syslog-message* [**priority** *priority-level*]

no action *action-label* **syslog**

Parameter Description

action-label: Label of an action.

facility *mnemonics*: Specifies the mnemonic of a log.

msg *syslog-message*: Specifies log content.

priority *priority-level*: Sets the priority of a log.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

The mnemonic of a log must consist of uppercase letters and underline, with a length of 4 to 32 characters. If the configured mnemonic exceeds the specified range, the **Action syslog** command fails.

Examples

The following example configures an action Test_2 for logging when the CPU usage of an entire device exceeds 95%.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_2
Hostname(config-applet)# event tag monitor_cpu sysmon cpu scope system
entry-op gt entry-val 95
Hostname(config-applet)# action 00 syslog msg "system busy !"
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.7 action wait

Function

Run the **action wait** command to configure an action for a policy by pausing a policy script.

Run the **no** form of this command to remove this configuration.

No action is configured for a policy by default.

Syntax

action *action-label* **wait** *wait-time*

no action *action-label* **wait**

Parameter Description

action-label: Label of an action.

wait-time: Wait time, in seconds. The value range is from 1 to 180.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a policy Test_1 by waiting for five seconds before running the **show arp** command.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_cli cli pattern "show arp" sync
yes
Hostname(config-applet)# action 00 cli command "enable"
Hostname(config-applet)# action 10 wait 5
Hostname(config-applet)# action 20 exit 1
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.8 commit

Function

Run the **commit** command to submit policy configuration.

No policy configuration is submitted by default.

Syntax

commit

Parameter Description

N/A

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a policy Test_1 and submits the policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag none-event none
Hostname(config-applet)# action 00 set var_for_test "Test_1 running"
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **rollback**

1.9 description

Function

Run the **description** command to configure the description of an SEM policy.

Run the **no** form of this command to remove this configuration

No description is configured for an SEM policy by default.

Syntax

description *string*

no description

Parameter Description

string: Text used to describe an SEM policy by the user.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

Modification to policy description takes effect immediately without submission.

Examples

The following example configures the description of an SEM policy as "Descrption_For_SEM_Applet".

```
Hostname> enable
Hostname# configure terminal
Hostname(config-applet)# description Descrption_For_SEM_Applet
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.10 event tag counter

Function

Run the **event tag counter** command to configure a counter monitoring event.

Run the **no** form of this command to remove this configuration.

No counter monitoring event is configured by default.

Syntax

event tag *event-name* [**correlate** { **and** | **andnot** | **or** }] **counter name** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **exit-op** *operator* **exit-val** *exit-value*

no event tag *event-name*

Parameter Description

event-name: Name of an event.

correlate { **and** | **andnot** | **or** }: Specifies the conditional relationship between the current event and the combination of all other events. **and** indicates a logical AND relation. **andnot** indicates a logical AND NOT relation. **or** indicates a logical OR relation.

name *counter-name*: Specifies the name of a monitored counter.

entry-op *operator*: Triggers a method used for comparison.

exit-op *operator*: Restores a comparison method.

operator indicates a method used for comparison. The value **eq** indicates equal. The value **ge** indicates greater than or equal to. The value **gt** indicates greater than. The value **le** indicates less than or equal to. The value **lt** indicates less than. The value **ne** indicates unequal to.

entry-val *entry-value*: Triggers a value used for comparison. The value range is from -2147483648 to 2147483647.

exit-val *exit-value*: Restore a value used for comparison. The value range is from -2147483648 to 2147483647.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- This command is used to configure a naming counter for SEM monitoring. The **action counter** command is run to modify the value of the naming counter.
- The **exit-op** and **exit-val** parameters are used to suppress frequent triggering of events. When an event is triggered, it becomes ineffective. If the comparison between the value of the naming counter and the value of the combination of the **exit-op** and **exit-val** parameters complies with the comparison method, the event is restored to effective status and can be triggered again.
- **correlate andnot** indicates a logical AND NOT relationship. For example, x **andnot** y means compliance with x but noncompliance with y.

Examples

The following example configures a counter monitoring policy Test_1 to trigger logging when the value of Test_Counter is greater than or equal to 10 and sets Test_Counter to 0 so that monitoring is restored when the value of Test_Counter is greater than 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_counter counter name
Test_Counter entry-op ge entry-val 10 exit-op gt exit-val 5
```

```
Hostname(config-applet)# action 10 counter name Test_Counter op set value
0
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **action counter**
- **smart manager applet**

1.11 event tag interface

Function

Run the **event tag interface** command to configure an interface monitoring event.

Run the **no** form of this command to remove this configuration.

No interface monitoring event is configured by default.

Syntax

event tag *event-name* [**correlate** { **and** | **andnot** | **or** }] **interface name** *interface-type interface-number* **parameter** { **link_down** | **link_up** }

no event tag *event-name*

Parameter Description

event-name: Name of an event.

correlate { **and** | **andnot** | **or** }: Specifies the conditional relationship between the current event and the combination of all the preceding events. **and** indicates a logical AND relation. **andnot** indicates a logical AND NOT relation. **or** indicates a logical OR relation.

interface-type interface-number: Interface type and interface number of a monitoring interface.

parameter { **link_down** | **link_up** }: Specifies the status of a monitoring interface. **link_down** indicates a down interface and **link_up** indicates an up interface.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

correlate andnot indicates a logical AND NOT relation. For example, x **andnot** y means compliance with x but noncompliance with y.

Examples

The following example configures logging when the status of GigabitEthernet0/1 changes to up.

```
Hostname> enable
Hostname(config)# smart manager applet Test_1
Hostname(config)# event tag monitor_interface interface parameter link_up
name GigabitEthernet0/1
Hostname(config-applet)# action 00 syslog msg "$_interface_name up"
Hostname(config-applet)# commit
Hostname(config-applet)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.12 event tag syslog

Function

Run the **event tag syslog** command to configure a log monitoring event.

Run the **no** form of this command to remove this configuration.

No log monitoring event is configured by default.

Syntax

event tag *event-name* [**correlate** { **and** | **andnot** | **or** }] **syslog** [**occurs** *num-occurrences*] **pattern** *regular-expression* [**period** *period-value*] [**priority** *priority-level*] [**skip** { **no** | **yes** }]

no event tag *event-name*

Parameter Description

event-name: Name of an event.

correlate { **and** | **andnot** | **or** }: Specifies the conditional relationship between the current event and the combination of all configured events. **and** indicates a logical AND relation. **andnot** indicates a logical AND NOT relation. **or** indicates a logical OR relation.

occurs *num-occurrences*: Specifies the number of occurrences that trigger an event. The value range is from 1 to 2147483647. The default value is **1**.

pattern *regular-expression*: Specifies a string for pattern match of log content.

period *period-value*: Specifies the expiry time of **occurs** in a command. An **occurs** operation that lasts for more than *period-value* times out. When the value of **occurs** is 1, this parameter is invalid, in seconds. The value range is from 1 to 2147483647. The default value is **30**.

priority *priority-level*: Sets the priority of a matched log.

skip { **no** | **yes** }: Specifies whether to ignore syslog. If the value is set to **yes**, a matched log is ignored. The default value is **no**.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- **correlate andnot** indicates a logical AND NOT relation. For example, x **andnot** y means compliance with x but noncompliance with y.
- To avoid event loop, logs sent by SEM, including logs suspended by the SEM scheduler and logs sent by Action Syslog, are ignored by the syslog detector without checking.
- Due to the limited space of a command line, the regular expression in the **pattern** parameter cannot include a question mark (?). To input, display and save configuration, use the ampersand and slash (&/) to replace the question mark (?) and use two ampersands (&&) to replace the ampersand (&). For example, a&/bc&&d represents a?bc&d.
- The **pattern** parameter can be used to add a sub-string of an event variable with the name pattern_name and the value regex in the (?<pattern_name>regex) format. The **pattern** parameter supports a maximum number of 16 sub-strings.

Examples

The following example configures a log monitoring event Test_1 to forcibly perform active/standby switchover of a device when "memory fail" is detected in the monitored log.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag monitor_log syslog pattern "memory fail"
Hostname(config-applet)# action 00 switchover
Hostname(config-applet)# commit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.13 event tag timer

Function

Run the **event tag timer** command to configure a timer monitoring event.

Run the **no** form of this command to remove this configuration.

No timer monitoring event is configured by default.

Syntax

event tag *event-name* [**correlate** { **and** | **andnot** | **or** }] **timer countdown time** *countdown-timer*

no event tag *event-name*

Parameter Description

event-name: Name of an event.

correlate { **and** | **andnot** | **or** }: Specifies the conditional relationship between the current event and the combination of all the preceding events. **and** indicates a logical AND relation. **andnot** indicates a logical AND NOT relation. **or** indicates a logical OR relation.

countdown time *countdown-timer*: Configures a time point when events can be triggered. *time-value* indicates the duration in which events can be triggered, in seconds. The value range is from 1 to 2147483.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- **correlate andnot** indicates a logical AND NOT relation. For example, x **andnot** y means compliance with x but noncompliance with y.

Examples

The following example configures a time point when an event Test_3 can be triggered: the duration in which the event can be triggered is 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_3
Hostname(config-applet)# event tag monitor_timer timer countdown time 10
Hostname(config-applet)# action 00 cli command "enable"
Hostname(config-applet)# action 10 cli command "clear arp-cache"
Hostname(config-applet)# commit
Hostname(config-applet)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.14 event tag track

Function

Run the **event tag track** command to configure a track monitoring event.

Run the **no** form of this command to remove this configuration.

No track monitoring event is configured by default.

Syntax

event tag *event-name* [**correlate** { **and** | **andnot** | **or** }] **track** [**state** { **down** | **up** }] [*track-id*]

no event tag *event-name*

Parameter Description

event-name: Name of an event.

correlate { **and** | **andnot** | **or** }: Specifies the conditional relationship between the current event and the combination of all the preceding events. **and** indicates a logical AND relation. **andnot** indicates a logical AND NOT relation. **or** indicates a logical OR relation.

state { **down** | **up** }: Specifies the status of a tracked entity. If this parameter is ignored, a tracked entity in the up or down status can trigger an event.

track-id: ID of a tracked entity. If this variable is ignored, all tracked entities are monitored.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- **correlate andnot** indicates a logical AND NOT relation. For example, x **andnot** y means compliance with x but noncompliance with y.
- Track-based events are categorized into the following types:
  - Monitoring the up or down status of a tracked object
  - Monitoring the up or down status of all tracked objects
  - Monitoring the up and down statuses of a tracked object
  - Monitoring the up and down statuses of all tracked objects
- Before a tracked object is monitored, this object must be configured in advance. Otherwise, users are notified of undetected object when SEM configures an event.

Examples

The following example configures an event Test_1 to print "track 1 up." when the status of tracked object 1 changes to up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag track_1 track 1 state up
Hostname(config-applet)# action 00 syslog msg "track 1 up."
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **smart manager applet**

1.15 list-config

Function

Run the **list-config** command to display the current policy configuration.

Syntax

list-config

Parameter Description

N/A

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of the Test_1 policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(sem-applet)# list-config

smart manager applet Test_1
  event tag monitor_time timer countdown time 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **commit**
- **rollback**

1.16 policy record

Function

Run the **policy record** command to enable the function of recording CLI command output and configure output size.

Run the **no** form of this command to remove this configuration.

The recording function is not enabled for CLI command action output by default.

Syntax

policy record [**per-instance** *record-size-per-policy*] [**per-policy** *record-size-per-policy*]

no policy record

Parameter Description

per-instance *record-size-per-policy*: Configures the size of CLI command output recorded each time a policy is triggered, in thousand bytes. The value range is from 1 to 50. The default value is **50**.

per-policy *record-size-per-policy*: Configures the total size of all CLI command output recorded when a policy is triggered, in thousand bytes. The value range is from 1 to 1024. The default value is **1000**.

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

- CLI command output is not recorded by default. After the **policy record** command is run, CLI command output will be recorded to the file system of a device. The output is recorded to the file /sem_record/policy_name/yyyy-mm-dd_hh-mm-ss_mspolicytriggerid.txt.
    - /sem_record/ is the general directory of all CLI command output and located in the root directory of the file system.
    - policy_name indicates the name of the policy and resides in the /sem_record/ directory. Each policy corresponds to a separate directory.
    - yyyy-mm-dd_hh-mm-ss_mspolicytriggerid.txt indicates the file name. The file name consists of the recording time and the ID of the triggered policy.

- The **more** command is run to display recorded content.
- When the size of the CLI command output generated during policy running exceeds the configured value of the **per-instance** *record-size-per-policy* parameter, the CLI command output starts to override the file from the header of the file.
- When the total size of the CLI command output files generated during running of a specific policy exceeds the configured value of the **per-policy** *record-size-per-policy* parameter, the earliest files start to be cleared until the total size of the CLI command output files complies with the configured value of **per-policy** *record-size-per-policy* parameter.
- The **smart manager policy record clean** command is run to clear CLI command output files in the file system.

Examples

The following example configures a Test_1 policy and records the CLI action output of the **enable** and **show arp** commands.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag none-event none
Hostname(config-applet)# action 00 cli command "enable"
Hostname(config-applet)# action 10 cli command "show arp"
Hostname(config-applet)# policy record
Hostname(config-applet)# commit
Hostname(config-applet)# exit
Hostname(config)# exit
Hostname# more /sem_record/Test_1/2010-01-01_01-00-00_1001.txt
                    SEM CLI RECORD FILE
SEM policy name: Test_1
SEM policy trigger id :1
SEM policy cli record time : Fri Jan 01 01:00:00 2010
=================================================
Hostname# enable
Hostname# show arp
Protocol  Address     Age(min)  Hardware       Type   Interface
Internet  6.6.6.6     21        0027.1994.e59b  arpa   VLAN 1
Internet  6.6.6.1     --        00d0.f822.33b3  arpa   VLAN 1
Total number of ARP entries: 2
Hostname#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **action cli**

1.17 rollback

Function

Run the **rollback** command to roll back the current policy configuration.

The policy rollback function is not enabled by default.

Syntax

rollback

Parameter Description

N/A

Command Modes

SEM configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example rolls back the configuration of the Test_1 policy.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_1
Hostname(config-applet)# event tag none-event none
Hostname(config-applet)# action 00 set var_for_test "Test_1 running"
Hostname(config-applet)# rollback
Hostname(config-applet)# exit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **commit**

1.18 show smart manager detector

Function

Run the **show smart manager detector** command to display detector information.

Syntax

show smart manager detector [**all** | *detector-name*] [**statistics**]

Parameter Description

all: Displays all detector information.

detector-name: Specific detector information.

statistics: Displays statistics of a detector.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays detector information.

```
Hostname> enable
Hostname# show smart manager detector all
No.  Name               Version
1    application         01.00
2    syslog             01.00
3    cli                01.00
4    counter             01.00
5    interface           01.00
6    sysmon             01.00
```

```
7    none                01.00
8    oir                 01.00
9    snmp                01.00
10   snmp-notification     01.00
11   timer               01.00
12   snmp-object          01.00
```

Table 1-1 Output Fields of the show smart manager detector all Command

Field	Description
No	Serial number displayed
Name	Detector name
Version	Detector version

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show smart manager history events

Function

Run the **show smart manager history events** command to display event history information.

Syntax

show smart manager history events [**detailed**] [**maximum** *number*]

Parameter Description

detailed: Displays detailed information.

maximum *number*: Configures the maximum number of events displayed. The value range is from 1 to 50.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays event history information.

```
Hostname> enable
Hostname# show smart manager history events detailed
No.   Job Id   Event Type    Time                  Policy name
1     927      timer         Thu Oct 21 13:59:54 2010  Test_1
      Class : default, Policy Type: applet
2     926      timer         Thu Oct 21 3:59:53 2010  Test_1
      Class : default, Policy Type: applet
3     925      timer         Thu Oct 21 13:59:52 2010  Test_1
      Class : default, Policy Type: applet
4     924      timer         Thu Oct 21 13:59:51 2010  Test_1
      Class : default, Policy Type: applet
5     923      timer         Thu Oct 21 13:59:50 2010  Test_1
      Class : default, Policy Type: applet
```

Table 1-2 Output Fields of the show smart manager history events detailed Command

Field	Description
No	Serial number displayed
Job Id	Instance ID of a policy
Event Type	Event type
Time	Time at which a policy instance is triggered
Policy name	Policy name
Class	Policy class
Policy Type	Policy type

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show smart manager policy all

Function

Run the **show smart manager policy all** command to display all policies and their submission information.

Syntax

show smart manager policy all

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Usage Guidelines

N/A

Default Level

15

Examples

The following example displays all policies and their submission information.

```
Hostname> enable
Hostname# show smart manager policy all
No.  Status       Policy Name
1    commit       Test_1
2    not commit    Test_2
```

Table 1-3 Output Fields of the show smart manager policy all Command

Field	Description
No.	Serial number displayed

Field	Description
Status	Policy submission information
Policy Name	Policy name

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show smart manager policy registered

Function

Run the **show smart manager policy registered** command to display registered policies.

Syntax

show smart manager policy registered [**class** *class-options*] [**event-type** *event-name*] [**policy** *policy-name*] [**statistics**]

Parameter Description

class *class-options*: Selects a policy class.

event-type *event-name*: Specifies an event type of a policy.

policy *policy-name*: Specifies a policy name.

statistics: Displays statistics of a registered policy.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays information of registered policies.

```
Hostname> enable
Hostname# show smart manager policy registered
No.  Name     Class   Type    Event Type      Time Registered
 1   Test_1   A      applet  timer          Thu Oct 21 13:46:16 2010
event_1: timer: watchdog time 1
 action 00 syslog msg "Action_00"
 action 10 wait 360
 action 20 syslog msg "Action_20"
```

Table 1-4 Output Fields of the show smart manager policy registered Command

Field	Description
No.	Serial number displayed
Name	Policy name
Class	Policy class
Type	Policy type
Event Type	Type of the first event of a policy
Time Registered	Time at which a policy is registered

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show smart manager version

Function

Run the **show smart manager version** command to display SEM versions.

Syntax

show smart manager version

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays SEM versions.

```
Hostname> enable
Hostname# show smart manager version
Smart Event Manager Version 1.0
Event Detectors:
name              version
timer             01.00
counter           01.00
interface         01.00
syslog            01.00
track             01.00
```

Table 1-5 Output Fields of the show smart manager version Command

Field	Description
name	Event name
version	Version No.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 smart manager applet

Function

Run the **smart manager applet** command to create an SEM policy.

Run the **no** form of this command to remove this configuration.

No SEM policy is created by default.

Syntax

smart manager applet *applet-name*

no smart manager applet *applet-name*

Parameter Description

applet-name: Name of an SEM policy. A policy name must consist of digits, letters, and underline.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- A policy includes the following configurations:
  - One or more events
  - One or more actions
  - Description of the policy
  - Trigger control information of the policy
- The **smart manager applet** command is run to enter the SEM configuration mode. In this mode, users can complete the following operations:
  - Configure events of the policy.

    Each event must be given a unique name based on the **tag** parameter. SEM arranges the events in the alphabetical order of the **tag** parameter.

- Configure actions of the policy.

  Each action must be given a unique label as well. SEM arranges the actions in the alphabetical order of the *label* parameter. When the policy is triggered, the actions are taken in the alphabetical order of the *label*.

- Configure description of the policy.
- Configure trigger control parameters of the policy.
- Submit the policy configuration.
- Roll back the policy configuration.
- Display the current policy configuration.

- In the SEM configuration mode, users can use environmental variables in the actions of the policy. The variables are divided into two types:
  - Global variable
  - Local variable

    The global variables can be defined by an event detector when an event occurs.

    The local variables can be defined based on actions during policy running.

Note

- Each policy corresponds to a class. The default class is **default**. Multiple policies can belong to the same class. A class is used to allocate thread resources to policies in the class and specify priorities of the policies in the class.
- Policy configuration cannot take effect immediately and must be submitted by running the **commit** command in the SEM configuration mode.
- When the policy configuration is submitted, their validity is checked. If the checking fails, the policy configuration fails to be submitted. In this case, the policy is not registered.
- If no event is configured for the policy, the policy cannot pass the validity check and the policy submission fails.
- If no action is configured for the policy, the policy can pass the validity check. However, no action is taken when the policy is triggered. Therefore, a warning is given during the policy submission.
- If users want to quit the changes to the policy configuration, run the **rollback** command to roll back the policy configuration.
- When multiple events are configured for a policy, the events are automatically arranged in the alphabetical order of tags and the events are juxtaposed. Other events, except the first event, are used as additional conditions of the first event. Except the first event, the relationship of the current event with the combination of all preceding events is referred to as the relationship of other events. The juxtaposition of the first event is ignored, and the default value of the juxtaposition is **and**.

Examples

The following example creates a CLI based policy and names the policy Test_A.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager applet Test_A
Hostname(config-applet)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 smart manager detector event-number

Function

Run the **smart manager detector event-number** command to configure upper limits of SEM detector parameters.

Run the **no** form of this command to remove this configuration.

By default, the maximum number of events configured for the counting detector, that of events for the interface detector, and that of events configured for the timer detector are 256, respectively.

Syntax

smart manager detector { **counter** | **interface** | **timer** | **track**} **event-number** *detector-number*

no smart manager detector { **counter** | **interface** | **timer** } **event-number**

Parameter Description

counter event-number *detector-number*: Configures the maximum number of events for a counter detector. The value range is from 1 to 256.

interface event-number *detector-number*: Configures the maximum number of events for an interface detector. The value range is from 1 to 256.

timer event-number *detector-number*: Configures the maximum number of events for a timer detector. The value range is from 1 to 256.

track event-number *detector-number*: Configures the maximum number of events for a track detector. It is not configured by default. The value range is from 1 to 128.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the maximum number of events for a timer detector to 128.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager detector timer event-number 128
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 smart manager global-variant number

Function

Run the **smart manager global-variant number** command to configure the maximum number of global variables of SEM.

Run the **no** form of this command to remove this configuration.

By default, the maximum number of global variables is **512**.

Syntax

smart manager global-variant number *global-variant-number*

no smart manager global-variant number

Parameter Description

global-variant-number: Maximum number of global variables. The value range is from 1 to 512.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the maximum number of global variables to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager global-variant number 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 smart manager policy

Function

Run the **smart manager policy** command to configure upper limits of SEM policy parameters.

Run the **no** form of this command to remove this configuration.

By default, the maximum number of actions in a policy is 64; the maximum numbers of policy detectors and registered policies are 128, respectively; and the maximum numbers of configured policies and policy delayed triggers are 256, respectively.

Syntax

smart manager policy { **action-number** *policy-number* | **config-number** *policy-number* | **event-number** *policy-number* | **register-number** *policy-number* | **trigger-delay-number** *policy-number* }

no smart manager policy { **action-number** | **config-number** | **event-number** | **register-number** | **trigger-delay-number** }

Parameter Description

action-number *policy-number*: Configures the maximum number of actions in a policy. The value range is from 1 to 64.

config-number *policy-number*: Configures the maximum number of policies. The value range is from 1 to 256.

event-number *policy-number*: Configures the maximum number of events that are detected by detectors. The value range is from 1 to 128.

register-number *policy-number*: Configures the maximum number of registered policies. The value range is from 1 to 128.

trigger-delay-number *policy-number*: Configures the maximum number of policy delayed triggers. The value range is from 1 to 256.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the maximum number of policy delayed triggers to 128.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager policy trigger-delay-number 128
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 smart manager record

Function

Run the **smart manager record** command to configure upper limits of SEM policy instance parameters.

Run the **no** form of this command to remove this configuration.

By default, the maximum number of policy instances is **50** and the maximum size of a policy file is **1024** KB.

Syntax

smart manager record { **size-of-instance** *record-number* | **size-of-policy** *record-number* }

no smart manager record { **size-of-instance** | **size-of-policy** }

Parameter Description

size-of-instance *record-number*: Configures the maximum number of policy instances. The value range is from 1 to 50.

size-of-policy *record-number*: Configures the maximum size of a policy file, in KB. The value range is from 1 to 1024.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the maximum number of policy instances to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager record size-of-instance 20
```

The following example sets the maximum size of a policy file to 200.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# smart manager record size-of-policy 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 smart manager schdulr

Function

Run the **smart manager schdulr** command to configure upper limits of SEM policy scheduler parameters.

Run the **no** form of this command to remove this configuration.

By default, the maximum number of wait policies of the scheduler and the maximum number of policies run by the scheduler are **128**, respectively.

Syntax

smart manager schdulr { **pending-number** *schdulr-number* | **running-number** *schdulr-number* }

no smart manager schdulr { **pending-number** | **running-number** }

Parameter Description

pending-number *schdulr-number*: Configures the maximum number of policies waiting in the queue of the scheduler. The value range is from 1 to 128.

running-number *schdulr-number*: Configures the maximum number of policies run by the scheduler. The value range is from 1 to 128.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example sets the maximum number of policies waiting in the queue of the scheduler and the maximum number of policies run by the scheduler to 12, respectively.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# smart manager schdulr running-number 12
Hostname(config)# smart manager schdulr pending-number 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 Intelligent Monitoring Commands

Command	Function
show fan	Display the fan information of a chassis.
show power	Display the power supply information.
show temperature	Display device temperature and threshold configuration.

1.1 show fan

Function

Run the **show fan** command to display the fan information of a chassis.

Syntax

show fan [[[*device-id*] *fan-id*] **detail** | **version**]

Parameter Description

device-id: Chassis ID of the fan tray to be displayed. This parameter is available only in VSU mode.

fan-id: ID of the fan tray to be displayed. IDs of all fan trays are displayed by default. In VSU mode, if a fan tray is specified but *device-id* is not specified, fans of the current chassis are displayed by default.

detail: Displays detailed information of fans. Except the content displayed by the **show fan** command, the rotating speed of the fans in each fan tray is displayed. For a faulty fan, its detailed fault information is displayed. The detailed information of all fan trays is displayed by default. If a fan tray ID is specified, only the detailed information of the specified fan tray is displayed.

version: Displays the version of a fan.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display fan information. If no parameter is specified in the **show fan** command, the model, serial number, operating status, and fan speed adjustment mode of all fan trays are displayed.
If a fan tray is faulty, the **show fan detail** command can be run to display fault cause of the fan tray.

Examples

The following example displays fan information.

```
Hostname> enable
Hostname# show fan
Fan id Type           Status    Hardware Version Serial Number
------ ---------------- ---------- ---------------- ---------------
1     M1SFAN I-F      ok        1.00           5555555555555
2     M1SFAN I-F      ok        1.00           6666666666666
```

Table 1-1 Output Fields of the show fan Command

Field	Description
Fan id	ID of a fan tray
Type	Fan type

Field	Description
Status	Status of a fan tray. A fan can be in one of the following statuses: ● **ok**: A fan runs normally. ● **no-present**: A fan tray is not in position. ● **fail**: At least one sub-fan stops rotating. ● **line fail**: Communication fails. ● **N/A**: Other errors.
Hardware-Version	Hardware version
Serial Number	Serial number of a fan

The following example displays detailed information of a fan.

```
Hostname> enable
Hostname# show fan detail
Card-type: RG-S6120-20XS4VS2QXS-L
Fan-id: 1
   Status:        ok
   Mode:          normal
   Fan-type:      M1SFAN I-F
   Serial Number:  5555555555555

   sub-fan-id  status  speed(rpm)  speed-level
   ----------  ------  ----------  ----------
   1          ok     7830       118
Fan-id: 2
   Status:        ok
   Mode:          normal
   Fan-type:      M1SFAN I-F
   Serial Number:  6666666666666

   sub-fan-id  status  speed(rpm)  speed-level
   ----------  ------  ----------  ----------
   1          ok     7980       118
---------
```

The following example displays detailed information of fan 1.

```
Hostname> enable
Hostname# show fan 1 detail
Chassis-type: S6120-20XS4VS2QXS
Fan-id: 1
   Status:        ok
   Mode:          normal
   Fan-type:      M1SFAN I-F
   Serial Number:  5555555555555
```

```
sub-fan-id  status  speed(rpm)  speed-level
----------  ------  ----------  ----------
1          ok     7125       108
```

Table 1-2 Output Fields of the show fan detail Command

Field	Description
Chassis-type	Device type
Fan id	ID of a fan tray
Status	Status of a fan tray. A fan can be in one of the following statuses: ● **ok**: A fan runs normally. ● **no-present**: A fan tray is not in position. ● **fail**: At least one sub-fan stops rotating. ● **line fail**: Communication fails. ● **N/A**: Other errors.
Mode	Fan mode. A fan can be in one of the following modes: ● **quiet**: Quiet mode. The rotating speed of a fan in the normal mode is higher than that of a fan in the quiet mode at the same level. ● **defined**: User-defined mode. The rotating speed of fans can be customized. ● **normal**: Normal mode.
Fan-type	Fan-type
Serial Numbe	Serial numbe of a fan
sub-fan-id	ID of a sub-fan
Status	Status of a sub-fan. A sub-fan can be in one of the following statuses (if there are multiple sub-fans, the corresponding fan tray fails when one sub-fan fails). ● **ok**: A sub-fan runs normally. ● **fail**: A sub-fan stops rotating.
speed(rpm)	Rotating speed, in revolutions per minute.
speed-level	Level of a rotating speed. The value range is from 1 to 255. A higher level indicates a greater rotating speed.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 show power

Function

Run the **show power** command to display the power supply information.

Syntax

show power [**version**]

Parameter Description

version: Displays serial number, hardware version No., and software version No. of each power supply.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays basic power supply information.

```
Hostname> enable
Hostname# show power
Power-id Power-type         Status    Hardware-Version Serial
Supply(W)
-------- -------------------- ---------- ----------------
------------------------------ ---------
1       RG-PA150I-F         ok        1.3            R253H1942130110
150
2       N/A               no-present N/A            N/A                          N/A
```

Table 1-3 Output Fields of the show power Command

Field	Description
Power-id	ID of a power supply

Field	Description
Power-type	Power supply type
Status	Status of a power supply: ● **no-present**: The power supply is not in position. ● **ok**: The power supply works normally. ● **off**: The power supply is powered off. ● **fail**: The power supply fails. ● **line-fail**: Communication fails.
Supply(W)	Power, in Watt
Hardware-Version	Hardware version
Serial	Serial number of a power supply

The following example displays power supply version information.

```
Hostname> enable
Hostname# show power version
Card-type: RG-S6120-20XS4VS2QXS-L
Power-id: 1
   Serial Number:     R253H1942130110
   Type:             RG-PA150I-F
   Hardware Version:   1.3
   Software Version:   N/A
   Temperature(C):    N/A
Power-id: 2
   Status:        no-present
```

Table 1-4 Output Fields of the show power version Command

Field	Description
Card-type	Device type
Power-id	ID of a power supply
Serial Number	Serial number of a power supply
Type	Power supply type
Hardware Version	Hardware version
Software Version	Software version
Temperature	Temperature of a power supply

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 show temperature

Function

Run the **show temperature** command to display device temperature and threshold configuration.

Syntax

show temperature

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display current temperature and temperature thresholds of a device.

Temperature thresholds include alarm threshold and hazard threshold.

- Alarm threshold: When the temperature of a device exceeds the alarm threshold, the active supervisor module generates a Syslog message and the alarm indicator on the panel turns yellow.
- Hazard threshold: It indicates the power-off temperature. When the temperature of a device exceeds the hazard threshold, the device is powered off automatically. In addition, the active supervisor module generates a Syslog message and the alarm indicator on the panel turns red.

Examples

The following example displays temperature and temperature thresholds of all devices.

```
Hostname> enable
Hostname# show temperature
Temperature:
-------------------------------------------------------------------------------
Slot    Temp_name    Warning       Shutdown      Current      Status
```

```
                  (Celsius)       (Celsius)     (Celsius)
-------------------------------------------------------------------------------
0       air_inlet       55             72             32          ok
0       board           60             77             39          ok
0       switch          90             102            55          ok
```

Table 1-5 Output Fields of the show temperature Command

Field	Description
Slot	Slot ID of a device
Temp_name	Name corresponding to a temperature point
Warning	Warning level of temperature, in °C
Shutdown	Critical level of temperature, in °C. This is the hazard threshold and power-off temperature of a device.
Current	Temperature value corresponding to this temperature, in °C
Status	Status of a temperature. A temperature can be in one of the following statuses: ● **ok**: Current temperature is within the normal range. ● **fail**: A temperature sensor fails. ● **warning**: Current temperature exceeds the alarm threshold of the warning level. ● **critical**: Current temperature exceeds the alarm threshold of the shutdown level.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1 NETCONF Commands

Command	Function
netconf enable	Enable the NETCONF function.
netconf max-sessions	Configure the maximum number of session connections supported by NETCONF.
netconf port	Configure the port ID of the NETCONF server.
netconf timeout	Configure the timeout time of the Edit-config operation in a NETCONF session.
netconf yang multi-revision	Enable the YANG module multi-version notification function of NETCONF.
show netconf session	Display all current session information of NETCONF.
show netconf statistics	Display global statistics of NETCONF.
show netconf yang file	Display all YANG files supported by a device.
show netconf yang node-path	Display all node paths supported by a device.
show netconf yang tree	Display all YANG model trees supported by a device.

1.1 netconf enable

Function

Run the **netconf enable** command to enable the NETCONF function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The NETCONF function is enabled by default.

Syntax

netconf enable

no netconf enable

default netconf enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the NETCONF function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no netconf enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 netconf max-sessions

Function

Run the **netconf max-sessions** command to configure the maximum number of session connections supported by NETCONF.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of session connections supported by NETCONF is **5** by default.

Syntax

netconf max-sessions *max-sessions-numbers*

no netconf max-sessions

default netconf max-sessions

Parameter Description

max-sessions *max-sessions-numbers*: Configures the maximum number of session connections supported by NETCONF. The value range is from 1 to 36.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of session connections supported by NETCONF to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# netconf max-sessions 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 netconf port

Function

Run the **netconf port** command to configure the port ID of the NETCONF server.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default port ID of the NETCONF server is **830**.

Syntax

netconf port *port-number*

no netconf port

default netconf port

Parameter Description

port-number: Port ID of the NETCONF server. The value range is from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the port ID of the NETCONF server to 5000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# netconf port 5000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 netconf timeout

Function

Run the **netconf timeout** command to configure the timeout time of the Edit-config operation in a NETCONF session.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default timeout time of the Edit-config operation in a NETCONF session is **120** seconds.

Syntax

netconf timeout *timeout*

no netconf timeout

default netconf timeout

Parameter Description

timeout: Timeout time, in seconds. The value range is from 50 to 1200.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The timeout time configured in this command for the Edit-config operation is not the duration between the delivery of an XML packet and the return of a reply. This timeout time counts from the completed processing of the XML packet is processed in NETCONF and the start of the business interaction.

Examples

The following example sets the timeout time of the Edit-config operation in a NETCONF session to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# netconf timeout 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 netconf yang multi-revision

Function

Run the **netconf yang multi-revision** command to enable the YANG module multi-version notification function of NETCONF.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The YANG module multi-version notification function of NETCONF is enabled by default.

Syntax

netconf yang multi-revision

no netconf yang multi-revision

default netconf yang multi-revision

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the YANG module multi-version notification function of NETCONF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no netconf yang multi-revision
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show netconf session

Function

Run the **show netconf session** command to display all current session information of NETCONF.

Syntax

show netconf session

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays all current session information of NETCONF.

```
Hostname> enable
Hostname# show netconf session
************************session information************************
                     Session count: 1
*****************************************************************
Session ID            : 25
Session version        : 1
Session transport      : netconf-ssh
Session login IP       : 172.30.31.17
Session login time     : 2019-07-16T05:59:50Z
Session in rpcs        : 0
Session in bad rpcs    : 0
Session out rpc errors  : 0
Session out notification: 0
Session out rpcs       : 0
Session out send fail   : 0
Session get           : 0
Session get config     : 0
Session edit config    : 0
Session copy config    : 0
Session delete config   : 0
Session close session   : 0
Session unsupport      : 0
Session lock_or_unlock  : 0
```

```
==============================================================
```

Table 1-1 Output Fields of the show netconf session Command

Field	Description
Session count	Total number of current sessions
Session ID	Session ID defined internally
Session version	Current NETCONF version No.
Session transport	Transmission protocol used in the current NETCONF connection. At present, only SSH is supported.
Session login IP	IP address of the connected objects in the current session
Session login time	Login time of the current session
Session in rpcs	Total number of correct RPC requests sent in the current session
Session in bad rpcs	Total number of incorrect RPC requests sent in the current session
Session out rpc errors	Total number of RPC replies with error returned in the current session
Session out notification	Total number of notifications output in the current session
Session out rpcs	Total number of RPC replies with success returned in the current session
Session out send fail	Total number of replies that failed to be sent in the current session
Session get	Total number of Get operations in the current session
Session get config	Total number of Get-Config operations in the current session
Session edit config	Total number of Edit-Config operations in the current session
Session copy config	Total number of Copy-Config operations in the current session
Session delete config	Total number of Delete-Config operations in the current session
Session close session	Total number of Close-Session operations in the current session
Session unsupport	Total number of requests unsupported in the current session
Session lock_or_unlock	Total number of Lock and Unlock operations in the current session

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show netconf statistics

Function

Run the **show netconf statistics** command to display global statistics of NETCONF.

Syntax

show netconf statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays global statistics of NETCONF.

```
Hostname> enable
Hostname# show netconf statistics
**********************statistics information**********************
Start time: 2019-07-11T01:37:45Z
       0 Bad hello packets
       2 Connected sessions
       1 Dropped sessions
      67 In rpcs
       0 In bad rpcs
       0 Out rpc errors
       0 Out notification
      67 Out rpcs
       0 Out send fail
      95 Get
      34 Get config
       0 Copy config
       0 Delete config
       0 Close session
```

```
        0 Unsupport
        0 Lock or unlock
==============================================================================
```

Table 1-2 Output Fields of the show netconf statistics Command

Field	Description
Start time	NETCONF start time
Bad hello packets	Number of hello packets with error
Connected sessions	Number of session connections (including dropped sessions)
Dropped sessions	Number of dropped sessions
In rpcs	Number of correct RPC requests in all sessions
In bad rpcs	Number of incorrect RPC requests in all sessions
Out rpc errors	Number of replies with error in all sessions
Out notification	Number of notifications in all sessions
Out rpcs	Number of correct replies in all sessions
Out send fail	Number of replies that failed to be sent in all sessions
Get	Number of Get operations in all sessions
Get config	Number of Get-Config operations in all sessions
Copy config	Number of Copy-Config operations in all sessions
Delete config	Number of Delete-Config operations in all sessions
Close session	Number of Close-Session operations in all sessions
Unsupport	Number of RPC requests unsupported in all sessions
Lock or unlock	Number of Lock and Unlock operations in all sessions

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show netconf yang file

Function

Run the **show netconf yang file** command to display all YANG files supported by a device.

Syntax

show netconf yang file

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays all YANG files supported by a device.

```
Hostname> enable
Hostname# show netconf yang file
============================================================
[YANG FILE]:  ietf-inet-types@2010-09-24.yang
[YANG FILE]:  ietf-netconf-acm.yang
[YANG FILE]:  ietf-netconf-monitoring@2010-10-04.yang
[YANG FILE]:  ietf-netconf.yang
[YANG FILE]:  ietf-yang-types@2013-07-15.yang
[YANG FILE]:  rg-access-control-list@2019-01-31.yang
[YANG FILE]:  rg-aggregateports@2016-01-01.yang
[YANG FILE]:  rg-bfd@2019-01-29.yang
[YANG FILE]:  rg-bridge@2019-02-01.yang
[YANG FILE]:  rg-cli@2018-12-28.yang
[YANG FILE]:  rg-device-management@2019-01-28.yang
[YANG FILE]:  rg-dhcp-relay@2019-01-28.yang
[YANG FILE]:  rg-dhcp-server@2016-06-06.yang
[YANG FILE]:  rg-erspan@2019-02-01.yang
[YANG FILE]:  rg-interfaces@2019-01-26.yang
[YANG FILE]:  rg-ip@2019-02-12.yang
[YANG FILE]:  rg-ipv4-unicast-routing@2019-01-26.yang
[YANG FILE]:  rg-ntp@2019-01-16.yang
[YANG FILE]:  rg-ospf@2019-02-14.yang
[YANG FILE]:  rg-packet-fields@2019-01-31.yang
[YANG FILE]:  rg-qos@2019-02-01.yang
```

```
[YANG FILE]:  rg-redundancy-management@2019-01-28.yang
[YANG FILE]:  rg-rns@2018-10-11.yang
[YANG FILE]:  rg-rpi@2019-02-12.yang
[YANG FILE]:  rg-snmp@2019-02-01.yang
[YANG FILE]:  rg-storm-control@2019-01-26.yang
[YANG FILE]:  rg-syslog@2018-10-11.yang
[YANG FILE]:  rg-sysmon@2019-02-26.yang
[YANG FILE]:  rg-system@2019-03-01.yang
[YANG FILE]:  rg-track@2018-10-11.yang
[YANG FILE]:  rg-tty-admin@2019-01-14.yang
[YANG FILE]:  rg-vxlan@2019-01-29.yang
============================================================
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show netconf yang node-path

Function

Run the **show netconf yang node-path** command to display all node paths supported by a device.

Syntax

show netconf yang node-path [*module-name*]

Parameter Description

module-name: Module name defined in a YANG file.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays all node paths supported by a device.

```
Hostname> enable
Hostname# show netconf yang node-path
==========================[rg-access-control-list]==========================
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-ipv4-network
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-ipv4-network-mask
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/source-ipv4-network
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/source-ipv4-network-mask
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-ipv6-network
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-ipv6-network-mask
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-ipv6-network-prefix-len
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/source-ipv6-network
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/source-ipv6-network-mask
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/source-ipv6-network-prefix-len
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/protocol
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/sport-op
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/sport
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/sport2
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/dport-op
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/dport
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/dport2
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/dscp
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/icmptype
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/icmpcode
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/precedence
```

```
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/tos
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/fragment
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/tcp-flag
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/vid
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/vid-inner
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-mac-address
/rg-access-control-list:access-lists/acl[acl-type
acl-name]/access-list-entries[rule-name]/destination-mac-address-mask
……
```

The following example displays node paths in the YANG file of the syslog module in a device.

```
Hostname> enable
Hostname# show netconf yang node-path rg-syslog
==========================[rg-syslog]==========================
/rg-syslog:syslog/log-server[ip]/ip
/rg-syslog:syslog/log-server[ip]/port
/rg-syslog:syslog/log-server-vrf[ip vrf]/ip
/rg-syslog:syslog/log-server-vrf[ip vrf]/vrf
/rg-syslog:syslog/log-server-vrf[ip vrf]/port
/rg-syslog:syslog/log-server-oob[ip mgmt]/ip
/rg-syslog:syslog/log-server-oob[ip mgmt]/mgmt
/rg-syslog:syslog/log-server-oob[ip mgmt]/port
```

Notifications

N/A

Common Errors

N/A

Platform Description

The node paths displayed by running this command are paths of the leaf/leaf-list nodes, and paths of other nodes are not displayed.

Related Commands

N/A

1.10 show netconf yang tree

Function

Run the **show netconf yang tree** command to display all YANG model trees supported by a device.

Syntax

show netconf yang tree [*module-name*]

Parameter Description

module-name: Model tree of a specified YANG file.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays all YANG model trees supported by a device.

```
Hostname> enable
Hostname# show netconf yang tree
==========================modules info==============================
ietf-inet-types, ietf-netconf-acm, ietf-netconf-monitoring, ietf-netconf,
ietf-yang-types,
rg-access-control-list, rg-aggregateports, rg-bfd, rg-bridge, rg-cli,
rg-device-management, rg-dhcp-relay, rg-dhcp-server, rg-erspan, rg-interfaces,
rg-ip, rg-ipv4-unicast-routing, rg-ntp, rg-ospf, rg-packet-fields,
rg-qos, rg-redundancy-management, rg-rns, rg-rpi, rg-snmp,
rg-storm-control, rg-syslog, rg-sysmon, rg-system, rg-track,
rg-tty-admin, rg-vxlan,
====================================================================
module: ietf-inet-types
=======================================================
module: ietf-netconf-acm
   +--rw nacm
      +--rw enable-nacm?            boolean <true>
      +--rw read-default?           action-type <permit>
      +--rw write-default?          action-type <deny>
      +--rw exec-default?           action-type <permit>
      +--rw enable-external-groups?   boolean <true>
      +--ro denied-operations        ietf-yang-types:zero-based-counter32
      +--ro denied-data-writes       ietf-yang-types:zero-based-counter32
      +--ro denied-notifications     ietf-yang-types:zero-based-counter32
      +--rw groups
     | +--rw group* [name]
     |    +--rw name        group-name-type
     |    +--rw user-name*   user-name-type
      +--rw rule-list* [name]
```

```
         +--rw name     string
         +--rw group*   union
         +--rw rule* [name]
            +--rw name               string
            +--rw module-name?        union <*>
            +--rw (rule-type)?
           | +--:(protocol-operation)
……
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A