Ruijie RG-S2915-L Series Switches

S2915-L_RGOS 11.4(1)B82

Command Reference

Document Version: V1.1
Date: 2023.03.15

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
- Skype: service_rj@ruijienetworks.com

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.

System Configuration Commands

1. Command Line Interface Commands
2. Basic Configuration Management Commands
3. Line Commands
4. File System Commands
5. SYS Commands
6. Time Range Commands
7. HTTP Service Commands
8. Syslog Commands
9. Security Log Commands
10. CWMP Commands
11. CA-MONITOR Commands
12. ZAM Commands
13. Module Hot-plugging/Unplugging Commands
14. Supervisor Module Redundancy Commands
15. PoE Management Commands
16. PKG-MGMT Commands
17. SF-APP Commands

1 Command Line Interface Commands

1.1 alias

Use this command to configure a command alias in global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

alias *mode command-alias original-command*

no alias *mode command-alias*

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

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias
command-alias	Command alias
original-command	Syntax of the command represented by the alias

Defaults Some commands in user or privileged EXEC mode have default alias.

Command Mode Global configuration mode.

Usage Guide The following table lists the default alias of the commands in privileged EXEC mode.

Alias	Actual Command
h	help
p	ping
s	show
u	undebug
un	undebug

The default alias cannot be removed by the **no alias exec** command.

After configuring the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use the **alias ?** command to list all the modes under which you can configure alias for commands.

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

The alias also has its help information that is displayed after * in the following format:

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

For example, in the privileged EXEC mode, the default alias s stands for show. You can enter s? to query the key words beginning with s and the help information of the alias.

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

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set sv stand for show version in the privileged EXEC mode, then:

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

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

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

The command alias also has its help information. For example, if the alias ia represents ip address in the interface configuration mode, then:

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

The above help information lists the parameters of **ip address** and shows the actual command name. You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

Configuration Examples

The following example uses def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1 in the global configuration mode:

```
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
```

Related Commands

Command	Description
show aliases	Displays the aliases settings.

Platform Description

N/A

1.2 privilege

Use this command to attribute the execution rights of a command to a command level in global configuration mode. Use the **no** form of this command to restore the default setting.

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

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

Parameter Description

Parameter	Description
mode	CLI mode of the command to which the execution rights are attributed.
all	Command alias
level *level*	Specifies the execution right levels (0–15) of a command or sub-commands
reset	Restores the command execution rights to its default level
command-string:	Command string to be authorized

Defaults N/A

Command Mode Global configuration mode.

Usage Guide The following table lists some key words that can be authorized by the **privilege** command in CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use the **privilege ?** command to list all CLI command modes that can be authorized.

Mode	Descripton
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode

Configuration Examples The following example sets the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
Hostname(config)#privilege exec level 1 reload
```

You can access the CLI window as level-1 user to usef the **reload** command:

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

<cr> You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
Hostname(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands 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
<cr>
```

Related Commands

Command	Description
enable secret	Sets the CLI-level password.

Platform Description N/A.

1.3 show aliases

Use this command to show all the command aliases or aliases in special command modes.

show aliases [*mode*]

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide This command displays the configuration of all aliases if no command mode is input.

Configuration Examples The following example displays the command alias in privileged EXEC mode:

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

Related Commands

Command	Description
alias	Sets a command alias.

Platform Description N/A.

2 Basic Configuration Management Commands

2.1 <1-99>

Use this command to restore the suspended Telnet Client session.

<1-99>

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to restore the suspended Telnet Client session. Hot keys (ctrl+shift+6 x) are used to exit the Telnet Client session creation. The **<1-99>** command is used to restore the session. If the session is created, you can use the **show session** command to display the session.

Configuration Examples The following example restores the suspended Telnet Client session.

```
Hostname# 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 banner exec

Use this command to configure a message to welcome the user entering user EXEC mode through the line. Use the **no** form of this command to restore the default setting.

banner exec *c message c*

no banner exec

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.

message	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol.
When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed.
The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

Configuration Examples The following example configures a welcome message.

```
Hostname(config)# banner exec $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 banner incoming

Use this command to configure a prompt message for reverse Telnet session. Use the **no** form of this command to remove the setting.
banner incoming *c message c*
no banner incoming

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol.
When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.

Configuration Examples The following example configures a prompt message for reverse Telnet session.

```
Hostname(config)# banner incoming $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.4 banner login

Use this command to configure a login banner. Use **no** form of this command to r remove the setting.
banner login *c message c*
no banner login

Parameter Description

Parameter	Description
c	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
message	Contents of the login banner

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command sets the login banner message, which is displayed at login. The system discards all the characters next to the terminating symbol.
When you log in to the device, a MOTD message (**banner motd**) is displayed at first, and then a login message (**banner login**). After you have logged in, an EXEC message (**banner exec**) or incoming message (**banner incoming**) is displayed. If it's a reverse Telnet session, an incoming message is displayed. Otherwise, the EXEC message is displayed.

Configuration Examples The following example configures a login banner.

```
Hostname(config)# banner login $ enter your password $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.5 banner motd

Use this command to set the Message-of-the-Day (MOTD) . Use the **no** form of this command to remove the setting.

banner [**motd**] *c message c*

no banner [**motd**]

Parameter Description

Parameter	Description
c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
message	Contents of an MOTD

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.

Configuration Examples The following example configures the MOTD.

```
Hostname(config)# banner motd $ hello,world $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.6 banner prompt-timeout

Use this command to configure the prompt-timeout message to notify timeout. Use the **no** form of this command to remove the setting.

banner prompt-timeout *c message c*

no banner prompt-timeout

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The system discards all the characters next to the terminating symbol.
When authentication times out, the banner prompt-timeout message is displayed.

Configuration Examples The following example configures the prompt-timeout message to notify timeout.

```
Hostname(config)# banner exec $ authentication timeout $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.7 banner slip-ppp

Use this command to configure the slip-ppp message for the SLIP/PPP session. Use the **no** form of this command to remove the setting.
banner slip-ppp *c message c*
no banner slip-pp

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure the slip-ppp message for the SLIP/PPP session. The system

discards all the characters next to the terminating symbol.
When the SLIP/PPP session is created, the slip-ppp message is displayed on the corresponding terminal.

Configuration Examples The following example configures the banner slip-ppp message for the SLIP/PPP session.

```
Hostname(config)# banner slip-ppp $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.8 boot configure

Use this command to modify the path for saving startup configurations and the corresponding file name.
boot config { **flash:filename** }
no boot config

Parameter Description

Parameter	Description
flash	Saves the startup configuration file in the extensible Flash.

Defaults By default, startup configuration file of a device is saved in **Flash:/config.text**

Command Mode Privileged EXEC mode

Usage Guide

⚠ The startup configuration file name follows a slash "/", for example, f**lash:/Hostname.text**.

⚠ The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **flash:/Hostname/Hostname.text** as examples, where the **flash:/Hostname** folder must exist. In master-slave mode, all device paths are required.

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

```
Hostname(config)#boot config flash:/Hostname.text
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.9 configure

Use this command to enter global configuration mode.

configure [**terminal**]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example enters global configuration mode.

```
Hostname# configure
Hostname(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 disable

Use this command to switch from privileged EXEC mode to user EXEC mode or lower the privilege level.

disable [*privilege-level*]

Parameter Description

Parameter	Description
privilege-level	Privilege level

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use this command to switch to user EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.

The privilege level that follows the **disable** command must be lower than the current level.

Configuration Examples The following example lowers the current privilege level of the device to level 10.

```
Hostname# disable 10
```

Related Commands

Command	Description
enable	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

Platform Description N/A

2.11 disconnect

Use this command to disconnect the Telnet Client session.

disconnect *session-id*

Parameter Description

Parameter	Description
session-id	Telnet Client session ID.

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to disconnect the Telnet Client session by setting the session ID.

Configuration Examples The following example disconnects the Telnet Client session by setting the session ID.

```
Hostname# disconnect 1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.12 enable

Use this command to enter privileged EXEC mode.

enable [*privilege-level*]

Parameter Description

Parameter	Description
privilege-level	Privilege level

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use this command to enter privileged EXEX mode from User EXEC mode. You can raise or lower the privilege level by specifying the privilege level.

Configuration Examples The following example lowers the privilege level to 14:

```
Hostname> enable 14

Password:
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 enable password

Use this command to configure passwords for different privilege levels. Use the **no** form of this command to restore the default setting.

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

no enable password [**level** *leve l*]

Parameter Description

Parameter	Description
password	Password for the user to enter the EXEC configuration layer
level	User's level.
0	The password is in plain text.

7 *encrypted-password*	The password is encrypted.

Defaults N/A

Command Mode Global configuration mode

Usage Guide No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device.
A valid password is defined as follows:

- Consists of 1-26 upper/lower case letters and numbers
- Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the password.

⚠ If an encryption type is specified and a plaintext password is entered, you cannot enter privileged EXEC mode. A lost password that has been encrypted using any method cannot be restored. In this case, you can only reconfigure the device password.

Configuration Examples The following example configures the password as **pw10**.

```
Hostname(config)# enable password pw10
```

Related Commands

Command	Description
enable secret	Sets the security password

Platform Description N/A

enable secret Sets the security password

2.14 enable secret

Use this command to configure a security password for different privilege levels. Use the **no** form of this command to restore the default setting.
enable secret [**level** *level*] { [**0**] *password* | [**5** | **8**] *encrypted-secret* }
no enable secret [**level** *level*]

Parameter Description

Parameter	Description
level	User's level.
0	(Optional) Specifies the plaintext password.
password	Password for the user to enter the EXEC configuration layer. The value is a string of 1 to 126 characters.

[**5** | **8**] *encrypted-secret*	Sets a password text encrypted by MD5 or SHA-256 irreversible encryption algorithm and saves it as an encrypted password after configuration. 5 indicates that the password is encrypted by MD5 algorithm and 8 indicates that the password is encrypted by SHA-256 algorithm.

Defaults N/A

Command Mode Global configuration mode

Usage Guide A password comes under two categories: "password" and "security". "Password" indicates a simple password, which can be set only for level 15. "Security" means a security password, which can be set for levels 0-15. If both types of passwords coexist in the system, no "password" type is allowed. If a "password" type password is set for a level other than 15, the system gives an alert and the password is automatically converted into a "security" password. If a "password" type password is set for level 15 and the same as a "security" password, an alert is given. The password must be encrypted, with simple encryption for "password" type passwords and security encryption for "security" type passwords.

Configuration Examples The following example configures the security password as **pw10**.

```
Hostname(config)# enable secret 0 pw10
```

Related Commands

Command	Description
enable password	Sets passwords for different privilege levels.

Platform Description N/A

2.15 enable service

Use this command to enable or disable a specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**.

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

Parameter Description

Parameter	Description
ssh-server	Enables SSH Server. IPv4 and IPv6 services are enabled at the same time.
telnet-server	Enables Telnet Server. IPv4 and IPv6 services are enabled at the same time.
web-server [**http	https	all**]	Enables HTTP Server. IPv4 and IPv6 services are enabled at the same time.

snmp-agent	Enables SNMP Agent. IPv4 and IPv6 services are enabled at the same time.

Defaults telnet-server, snmp-agent and web-server are enabled. ssh-server is disabled.

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable a specified service. Use the **no enable service** command to disable the specified service.

> The **enable service web-server** command is followed by three optional keywords: [http | https | all]. If the command is followed by no keyword or by **all**, the command enables http and https services. Followed by **http**, the command enables http service only. Followed by **https**, the command enables https service only.

Configuration Examples The following example enables the SSH Server.

```
Hostname(Config)# enable service ssh-sesrver
```

Related Commands

Command	Description
show service	Displays the service status in the current system.

Platform Description N/A

2.16 end

Use this command to return to privileged EXEC mode.

end

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All modes except privileged EXEC mode

Usage Guide Use this command to return to privileged EXEC mode.

Configuration The following example returns to privileged EXEC mode.

Examples

```
Hostname#con
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Hostname#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 exec-banner

Use this command to enable display of the EXEC message on a specific line. Use the **no** form of this command to restore the default setting.

exec-banner

no exec-banner

Parameter Description

Parameter	Description
N/A	N/A

Defaults The EXEC message is displayed on all lines by default.

Command Mode LINE configuration mode

Usage Guide After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

This command does not work for the banner incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration Examples The following example disables display of the EXEC message on line VTY 1.

```
Hostname(config)# line vty 1
Hostname(config-line)no exec-banner
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

2.18 exec-timeout

Use this command to configure connection timeout for this device in LINE mode. Use the **no** form of this command to restore the default setting and the connection never expires.

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

no exec-timeout

Parameter Description

Parameter	Description
minutes	Timeout in minutes.
seconds	(Optional) Timeout in minutes

Defaults The default is 10 minutes.

Command Mode Line configuration mode

Usage Guide If there is no input or output for this connection within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration Examples The following example sets the connection timeout to 5’30’’.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.19 execute

Use this command to execute a command on the file.

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

Parameter Description

Parameter	Description
filename	Specifies the file path.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example executes a command to configure an IP address for the specified interface.

```
Hostname#execute flash:mybin/config.text
executing script file mybin/config.text ......
executing done
Hostname#config
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.21.158 24
Hostname(config-if-GigabitEthernet 0/1)#end
*Sep 29 23:35:49: %SYS-5-CONFIG_I: Configured from console by console
Hostname#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 exit

Use this command to return to the upper configuration mode.

exit

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration The following example returns to the upper configuration mode.

Examples

```
Hostname#con
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Hostname#con
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#exit
Hostname(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console
Hostname#exit

Press RETURN to get started
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.21 help

Use this command to display the help information.

help

Parameter Description

Parameter	Description
N/A	N/A

Defaults Any mode

Command Mode

Usage Guide This command is used to display brief information about the help system. You can use ”?” to display all commands or a specified command with its parameters.

Configuration Examples The following example displays brief information about the help system.

```
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 available commands in interface configuration mode.

```
Hostname(config-if-GigabitEthernet 0/0)#?
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 configuration example is for reference only. The actual device configuration prevails.

The following example displays the parameters of a specified command.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.22 hostname

Use this command to specify or modify the hostname of a device**.**

hostname *name*

Parameter Description

Parameter	Description
name	Device hostname, string, number or hyphen, up to 63 characters.

Defaults The default is Hostname.

Command Mode Global configuration mode

Usage Guide This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.

Configuration Examples The following example configures the hostname of the device as Hostname.

```
Hostname(config)# hostname Hostname
```

```
Hostname(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.23 ip telnet source-interface

Use this command to configure the IP address of an interface as the source address for Telnet connection.

ip telnet source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Configures the IP address of the interface, including AP port, Gi port, Loopback port, null port and VLAN port, as the source address for Telnet connection.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the IP address of an interface as the source address for global Telnet connetction. When using the telnet command to log in a Telnet server, apply the global setting if no source interface or source address is specified. Use the **no ip telnet source-interface** command to restore it to the default setting.

Configuration Examples The following example configures the IP address of the *Loopback1* interface as the source address for global Telnet connection.

```
Hostname(Config)# ip telnet source-interface Loopback 1
```

Related Commands

Command	Description
telnet	Logs in a Telnet server.

Platform Description N/A

2.24 lock

Use this command to set a temporary password for the terminal.

lock

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide You can lock the terminal interface and maintain the session continuity to prevent access to the interface by setting a temporary password. Take the following steps to lock the terminal interface:

- Enter the **lock** command, and the system will prompt you for a password:
- Enter the password, which can be any character string. The system will prompt you to confirm the password, clear the screen, and display the "Locked" information.
- To access the terminal, enter the preset temporary password.
- To lock the terminal, run the **lockable** command in line configuration mode and enable terminal locking in the corresponding line.

Configuration Examples The following example locks a terminal interface.

```
Hostname(config-line)# lockable
Hostname(config-line)# end
Hostname# lock
Password: <password>
Again: <password>
Locked
Password: <password>
Hostname#
```

Related Commands

Command	Description
lockable	Supports terminal locking in the line.

Platform Description N/A

2.25 lockable

Use this command to support the **lock** command at the terminal. Use the **no** form of this command to

restore the default setting.

lockable

no lockable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode LINE configuration mode

Usage Guide This command is used to lock a terminal interface in the corresponding line. To lock the terminal, run the lock command in EXEC mode. Run the **lockable** command before running the **lock** command.

Configuration Examples The following example enables terminal locking at the console port and locks the console.

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

Related Commands

Command	Description
lock	Locks the terminal.

Platform Description N/A

2.26 login

Use this command to enable simple login password authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login

no login

Parameter Description

Parameter	Description
N/A	N/A

Defaults Login is disabled for console and enabled for AUX, TTY and VTY by default.

Command Mode Line configuration mode

Usage Guide If the AAA security server is inactive, this command enables simple password authentication at login. The password is configured for a VTY or console interface.

Configuration Examples The following example sets a login password authentication on VTY..

```
Hostname(config)# no aaa new-model
Hostname(config)# line vty 0
Hostname(config-line)# password 0 normatest
Hostname(config-line)# login
```

Related Commands

Command	Description
password	Configures the line login password

Platform Description N/A

2.27 login access non-aaa

Use this command to configure non-AAA authentication on line when AAA is enabled. Use the **no f**orm of this command to restore the default setting.

login access non-aaa

no login access non-aaa

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures VTY line authentication with AAA enabled.

```
Hostname(config)#log access non-aaa
Hostname(config)#aaa new-model
Hostname(config)#line vty 0 4
Hostname(config-line)#login local
```

```
Hostname(config-line)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 login authentication

If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate login authentication method list. Use the **no** form of this command to restore the default setting.

login authentication { **default |** *list-name* }

no login authentication { **default** | *list-name* }

Parameter Description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list

Defaults Default authentication is used when AAA is enabled.

Command Mode Line configuration mode

Usage Guide

Configuration Examples The following example associates the method list on VTY and perform login authentication on a radius server.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa authentication login default radius
Hostname(config)# line vty 0
Hostname(config-line)# login authentication default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication login	Configures the login authentication method list.

Platform Description N/A

2.29 login local

Use this command to enable local user authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login local

no login local

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Line configuration mode

Usage Guide If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the **username** command.

Configuration Examples The following example sets local user authentication on VTY.

```
Hostname(config)# no aaa new-model
Hostname(config)# username  test password 0 test
Hostname(config)# line vty 0
Hostname(config-line)# login local
```

Related Commands

Command	Description
username	Configures local user information.

Platform Description N/A

2.30 login privilege log

Use this command to log privilege change. Use the **no** form of this command to restore the default setting.

login privilege log

no login privilege log

Parameter Description

Parameter	Description
N/A	N/A

Defaults This command is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the function of logging privilege change.

```
Hostname(config)# login privilege log
```

The following example displays the log of privilege change failure.

```
Hostname>enable 10

Password:
Password:
Password:

% Access denied
Hostname>
*Sep 10 11:34:19: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 10
from console failed
```

The following example displays the log of privilege change success.

```
Hostname>enable 10

Password:
Hostname#
*Sep 10 11:34:20: %SYS-5-PRIV_AUTH_SUCCESS: Authentication to privilege level
10 from console success
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.31 motd-banner

Use this command to enable display of the MOTD message on a specified line. Use the **no** form of this command to restore the default setting.

motd-banner

no motd-banner

Parameter Description

Parameter	Description

N/A	N/A

Defaults The MOTD message is displayed on all lines by default.

Command Mode Line configuration mode

Usage Guide After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

This command does not work for the incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration Examples The following example disables display of the MOTD message on VTY 1.

```
Hostname(config)# line vty 1
Hostname(config-line)no motd-banner
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.32 password

Use this command to configure a password for line login, run the **password** command. Use the **no** form of this command to restore the default setting.

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

no password

Parameter Description

Parameter	Description
password	Password for remote line login
0	The password is in plain text.
7 *encrypted-password*	The password is encrypted.

Defaults N/A

Command Mode Line configuration mode

Usage Guide

Configuration Examples The following example configures the line login password as "red".

```
Hostname(config)# line vty 0
Hostname(config-line)# password red
```

Related Commands

Command	Description
login	Moves from user EXEC mode to privileged EXEC mode or enables a higher level of authority.

Platform Description N/A

2.33 prompt

Use this command to set the **prompt** command. Use the **no** form of this command to restore the default setting.

prompt string

Parameter Description

Parameter	Description
string	Character string of the **prompt** command, containing up to 32 letters.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If no prompt string is configured, the system name applies and varies with the system name. The **prompt** command is valid only in EXEC mode.

Configuration Examples The following example sets the prompt string to test.

```
Hostname(config)# prompt test
Hostname(config)# endtest
test
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.34 secret

Use this command to set a password encrypted by irreversible MD5 for line login. Use the **no** form of this command to restore the default setting.

secret { [**0**] *password* | **[5 | 8]** *encrypted-secret* }

no secret

Parameter Description

Parameter	Description
0	(Optional) sets the plaintext password text and encrypts it with irreversible MD5 after configuration.
password	Sets the password plaintext of a remote user' line, a string ranging from 1 to 25 characters.
[5 | 8] *encrypted-secret*	Sets a password text encrypted by MD5 or SHA-256 irreversible encryption algorithm and saves it as an encrypted password after configuration. 5 indicates that the password is encrypted by MD5 algorithm and 8 indicates that the password is encrypted by SHA-256 algorithm.

Defaults N/A

Command mode Line configuration mode

Usage Guide This command is used to set a password encrypted by irreversible MD5 or SHA-256 algorithm that is authenticated by a remote user through line login.

⚠ If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1st, 3rd and 8th characters of the password text must be $.

In general, the encryption type does not need to be specified as 5 except when the encrypted password is copied and pasted.

Line mode allows configuration of both "password" and "secret" types passwords at the same time. When the two passwords are the same, the system will send alert notification but the configuration will be permitted. When the system is configured with the two passwords, if the user enters a password that does not match the "secret" type password, it will not continue to match the "password" type password and login fails, enhancing security for the system password.

Configuration Examples The following example sets the password encrypted by irreversible MD5 for line login to vty0.

```
Hostname(config)# line vty 0
Hostname(config-line)# secret vty0
```

The following displays the encryption outcome by running the **show** command.

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

Related Commands

Command	Description
login	Sets simple password authentication on the interface as the login authentication mode

Platform Description N/A

2.35 session-timeout

Use this command to configure the session timeout for a remote terminal. Use the **no** form of this command to restore the default setting and the session never expires.

session-timeout *minutes* [**output**]

no session-timeout

Parameter Description

Parameter	Description
minutes	Timeout in minutes. The value range if from 0 to 35791.
output	Regards data output as the input to determine whether the session expires.

Defaults The default timeout is 0.

Command Mode LINE configuration mode

Usage Guide If no input or output in current LINE mode is found on the remote terminal for the session within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration Examples The following example specifies the timeout as 5 minutes.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.36 show boot config

Use this command to display the path for saving startup configurations and the corresponding file name.

show boot config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the path for saving startup configurations and the corresponding file name.

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

Related Commands

Command	Description
flash:/Hostname.text	The path and name of saved startup configuration file.

Platform Description N/A

2.37 show debugging

Use this command to display debugging state.

show debugging

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays debugging state.

```
Hostname#show debugging
```

```
debug fw-group detect intf-state
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.38 show line

Use this command to display the configuration of a line.

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

Parameter Description

Parameter	Description
console	Displays the configuration of a console line.
vty	Displays the configuration of a vty line.
line-num	Number of the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of a console port.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.39 show reload

Use this command to display the system restart settings.

show reload

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

Configuration Examples The following example displays the restart settings of the system.

```
Hostname# show reload
Reload scheduled in 595 seconds.
At 2003-12-29 11:37:42
Reload reason: test.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.40 show running-config

Use this command to display how the current device system is configured..

show running-config

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.41 show service

Use this command to display the service status.

show service

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays whether the service is enabled or disabled.

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

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

2.42 show sessions

Use this command to display the Telnet Client session information.

show sessions

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide Telnet Client session information includes the VTY number and the server IP address.

Configuration Examples The following example displays the Telnet Client session information.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.43 show startup-config

Use this command to display the device configuration stored in the Non Volatile Random Access Memory (NVRAM).

show startup-config

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The device configuration stored in the NVRAM is executed while the device is starting.
On a device that does not support **boot config**, **startup-config** is contained in the default configuration file **/config.text** in the built-in flash memory.

Configuration Examples N/A

Related Commands

Command	Description
boot config	Sets the name of the boot configuration file.

Platform Description N/A

2.44 show this

Use this command to display effective configuration in the current mode.
show this

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All modes.

Usage Guide The configuration in the following range modes cannot be displayed. If the **show this** command is run, the outcome is NULL.

1. Use the **line** *first-line last-line* command to configure lines in a continuous group and enter LINE configuration mode.
2. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode.
3. Use the **interface range** command to configure interfaces and enter interface range configuration mode.

In **vlan range** or **interface range** mode, if the number of VLANs or interfaces exceeds 50, the

configuration of the first 50 VLANs or interfaces will be displayed.

Configuration Examples

Use this command to display effective configuration on interface fastEthernet 0/1.

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

Use this command to display configuration on interface VLAN 1-3.

```
Hostname(config-if-range)#show this

Building configuration...
!
interface VLAN 1
 ip address dhcp
interface VLAN 2
 ip address 1.1.1.1 255.255.255.0
interface VLAN 3
 ip address 3.3.3.3 255.255.255.0
!
end
Hostname(config-if-range)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.45 speed

Use this command to set the speed at which the terminal transmits packets. Use the **no** form of this command to restore the default setting.

speed *speed*

no speed

Parameter

Parameter	Description

Description

speed	Transmission rate (bps) on the terminal. For serial ports, optional rates include 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.

Defaults The default is 9600.

Command Mode Global configuration mode

Usage Guide This command is used to set the speed at which the terminal transmits packets.

Configuration Examples The following example sets the rate of the serial port to 57600 bps.

```
Hostname(config)# line console 0
Hostname(config-line)# speed 57600
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.46 telnet

Use this command to log in a server that supports telnet connection.

telnet *host* [*port*] [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]

Parameter Description

Parameter	Description
host	The IP address of the host or host name you want to log in.
port	Selects the TCP port number for login, 23 by default.
/source	Specifies the source IP address or source interface used by the Telnet client.
ip A.B.C.D	Specifies the source IPv4 address used by the Telnet client.
ipv6 X:X:X:X::X	Specifies the source IPv6 address used by the Telnet client.
interface *interface-name*	Specifies the source interface used by the Telnet client.

Defaults N/A

Command Mode User EXEC mode

Usage Guide

Configuration Examples The following example sets telnet to IPv6 address 2AAA:BBBB::CCCC.

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

Related Commands

Command	Description
ip telnet source-interface	Specifies the IP address of the interface as the source address for Telnet connection.
show sessions	Displays the currently established Telnet sessions.
exit	Exits current connection.

Platform Description N/A

2.47 username

Use this command to set a local username and optional authorization information.. Use the **no** form of this command to restore the default setting.

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

no username *name*

Parameter Description

Parameter	Description
name	Username
login mode	Sets the login mode.
aux	Sets the login mode to aux.
console	Sets the login mode to console.
ssh	Sets the login mode to ssh.
telnet	Sets the login mode to telnet.
online amount *number*	Sets the amount of users online simultaneously.
permission *oper-mode path*	Sets the permission on the specified file. *op-mode* refers to the operation mode and *path* to the file or the directory path.
privilege *privilege-level*	Sets the privilege level, in the range from 0 to 15.
reject remote-login	Confines the account to remote login.
web-auth	Confines the account to web authentication.
pwd-modify	Allows the web authentication user of this account to change the password. It works only when the **web-auth** command is configured.
nopassword	The account is not configured with a password.
password [**0**	**7**] *text-string*	If the password type is 0, the password is in plain text. If the type is 7,

	the password is encrypted. The password is in plain text by default.
secret [**0** | **5**] *text-string*	If the password type is 0, the password is in plain text. If the type is 5, the password is encrypted. The password is in plain text by default.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to establish a local user database for authentication.

If encryption type is 7, the cipher text you enter should contain seven characters to be valid. In general, do not set the entryption type 7.
Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.

Configuration Examples The following example configures a username and password and binds the user to level 15.

```
Hostname(config)# username test privilege 15 password 0 pw15
```

The following example configures the username and password exclusive to web authentication.

```
Hostname(config)# username user1 web-auth password 0 pw
```

The following example configures user test with read and write permissions on all files and directories.

```
Hostname(config)# username test permission rw /
```

The following example configures user test with read, write and execute permissions on all files and directories except the confix.text file.

```
Hostname(config)# username test permission n /config.text
Hostname(config)# username test permission rwx /
```

Related Commands

Command	Description
login local	Enables local authentication

Platform Description N/A

2.48 username import

Use this command to import user information from the file.
username import *filename*

Parameter Description

Parameter	Description
filename	The file name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to import user information from the file.

Configuration Examples The following example imports user information from the file.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.49 username export

Use this command to export user information to the file.

username export *filename*

Parameter Description

Parameter	Description
filename	The file name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to export user information to the file.

Configuration Examples The following example exports user information to the file.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.50 write

Use this command to save **running-config** at a specified location.

write [**memory | terminal**]

Parameter Description

Parameter	Description
memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
terminal	Displays the system configuration, which is equivalent to **show running-config**.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations.

The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists;

The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device, and the device has not been loaded when you run the **write** [**memory**] command.

Configuration Examples The following example saves **running-config** at a specified location.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.51 zcm

Use this command to enable and disable the zero configuration function.

zcm { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the zero configuration function.
disable	Disables the zero configuration function.

Defaults The zero configuration function is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide

- The zero configuration function is applicable to the ACS solution only.
- The zero configuration function is applicable to standalone systems only.
- With the zero configuration function, DHCP Snooping Trust is enabled only on the last two electrical ports and all SFP ports of the device by default, regardless of whether the device supports the MGMT port.
- Enabling and disabling the zero configuration function will delete the startup configuration file of the device and trigger device restart.

Configuration Examples The following example enables the zero configuration function.

```
Hostname# zcm enable
%% Warning: After switching mode the device will automatically restart!
% Do you want to switch to zero configuration mode? [yes/no]:y
*Sep 29 12:36:20: %ZCM-5-MODE_SWITCH: The device is reloading due to zero or
   non-zero configuration mode switch.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3 Line Commands

3.1 absolute-timeout

Use this command to set the absolute timeout period. Use the **no** form of this command to restore the default setting.

absolute-timeout *minutes*

no absolute-timeout

Parameter Description

Parameter	Description
minutes	Sets the absolute timeout period, in the range from 0 to 60.

Defaults No absolute timeout period is set by default.

Command Mode LINE configuration mode

Usage Guide If the absolute timeout period is configured, the line is disconnected once the timeout timer expires, Before the terminal logs out, a message is displayed to prompt the remaining time.

```
Terminal will be login out after 20 second
```

Configuration Examples The following example sets the timeout period for the line between two consoles to 2 minutes.

```
Hostname(config)# line console 0
Hostname(config-line)#absolute-timeout 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.2 access-class

Use this command to control login into the terminal through IPv4 ACL. Use the **no** form of this command to restore the default setting.

access-class { *access-list-number* | *access-list-name* } { **in | out** }

no access-class { *access-list-number* | *access-list-name* } { **in | out** }

Parameter

Parameter	Description

Description

access-list-number	Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699.
access-list-name	Specifies the ACL name.
in	Filters the incoming connections.
out	Filters the outgoing connections.

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example uses ACL 20 to filter the incoming connections in line VTY 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)access-list 20 in
```

The following example uses the ACL named “test” to filter the outgoing connections in line VTY 6 7.

```
Hostname(config)# line vty 6 7
Hostname(config-line)access-list test out
```

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.3 accounting commands

Use this command to enable command accounting in the line. Use the **no** form of this command to restore the default setting.

accounting commands *level* { **default** | *list-name* }

no accounting commands *level*

Parameter Description

Parameter	Description
level	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
default	Default authorization list name.
list-name	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA command accounting first, and then apply it on the line.

Configuration Examples The following example enables command accounting in line VTY 1 and sets the command level to 15.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting commands 15 default start-stop group tacacs+
Hostname(config)# line vty 1
Hostname(config-line)# accounting commands 15 default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 accounting exec

Use this command to enable user access accounting in the line. Use the **no** form of this command to restore the default setting.

accounting commands *level* { **default** | *list-name* }

no accounting commands *level*

Parameter Description

Parameter	Description
level	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
default	Default authorization list name.
list-name	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA EXEC accounting first, and then apply it on the line.

Configuration Examples The following example enables user access accounting in line VTY 1.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 activation-character

Use this command to set the ASCII value of the character for activating the terminal session. Use the **no** form of this command to restore the default setting.

activation-character *ascii-value*

no activation-character

Parameter Description

Parameter	Description
ascii-value	Sets the ASCII value of the character for activating the terminal session, in the range from 0 to 127.

Defaults The default is CR (ASCII: 0x0D).

Command Mode LINE configuration mode

Usage Guide If the current line is configured with the **autoselect** function, *ascii-value* must be set to 0x0D.

Configuration Examples The following example configures Ctrl+Y (ASCII: 25) for activating the terminal session.

```
Hostname(config)#line console 0
Hostname(config-line)#activation-character 25
Hostname(config-line)#end
Hostname#exit

Press CTRL+y to get started

Hostname>
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

3.6 authorization commands

Use this command to enable authorization on commands, Use the **no** form of this command to restore the default setting.

authorization commands *level* { **default** | *list-name* }

no authorization commands *level*

Parameter Description

Parameter	Description
level	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
default	Default authorization list name,
list-name	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA authorization first, and then apply it on the line.

Configuration Examples The following example enables authorization on commands of level 15 in line VTY 1.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa authorization commands 15 default group tacacs+
Hostname(config)# line vty 1
Hostname(config-line)# authorization commands 15 default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 authorization exec

Use this command to enable EXEC authorization for the line. Use the **no** form of this command to

restore the default setting.

authorization { **default** | *list-name* }

no authorization exec

Parameter Description

Parameter	Description
default	Default authorization list name,
list-name	Optional list name.

Defaults This function is disabled by default,

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA EXEC authorization first, and then apply it on the line.

Configuration Examples The following example performs EXEC authorization to line VTY 1.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa authorization exec default group radius
Hostname(config)# line vty 1
Hostname(config-line)# authorization exec default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 autocommand

Use this command to enable automatic command execution. Use the **no** form of this command to restore the default setting.

autocommand *autocommand-string*

no autocommand

Parameter Description

Parameter	Description
autocommand-string	Enables automatic command execution.

Defaults This function is disabled by default.

Command LINE configuration mode

Mode

Usage Guide This command is used to enable the dumb terminal to log in to the specified host through Telnet or to obtain the specified app-based terminal service.

Configuration Examples The following example enables automatic command execution and connects to line vty 0.

```
Hostname(config)# line vty 0
Hostname(config-line)# autocommand telnet 192.168.21.100

//Initiates connection to line vty 0:
Trying 192.168.21.100, 23...

Hostname#show users
Line           User        Host(s)             Idle      Location
---------------- ------------ -------------------- ----------
   ------------------
  0 con 0      ---         idle              00:01:31   ---
*  1 vty 0      ---         idle              00:00:00   192.168.21.200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 clear line

Use this command to clear connection status of the line.

clear line { **console** *line-num* | **vty** *line-num* **|** *line-num* }

Parameter Description

Parameter	Description
console	Clears connection status of the console line.
vty	Clears connection status of the virtual terminal line.
line-num	Specifies the line to be cleared.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear connection status of the line and restore the line to the unoccupied

status to create new connections.

Configuration Examples The following example clears connection status of line VTY 13. The connected session on the client (such as Telnet and SSH) in the line is disconnected immediately.

```
Hostname# clear line vty 13
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 databits

Use this command to set the databit number for every character on the async line in flow communication mode. Use the **no** form of this command to restore the default setting.

databits *bit*

no databits

Parameter Description

Parameter	Description
bit	Sets the databit number of every character, in the range from 5 to 8.

Defaults The default is 8.

Command Mode LINE configuration mode

Usage Guide The async line device generates 7 databits with parity check in flow communication mode. If parity check is enabled, the databit number is 7. Otherwise, the databit number is 8. The databit number may set to 5 or 6 on the earlier device.

Configuration Examples The following example sets the databit number for every character on the async line in flow communication mode to 7.

```
Hostname(config)# line console 0
Hostname(config-line)#databits 7
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 disconnect-character

Use this command to set the hot key that disconnects the terminal service connection. Use the **no** form of this command to restore the default setting.

disconnect-character *ascii-value*

no disconnect-character

Parameter Description

Parameter	Description
ascii-value	ASCII decimal value of the hot key that disconnects the terminal service connection, in the range from 0 to 255.

Defaults The default hot key is **Ctrl+D** and the ASCII decimal value is 0x04.

Command Mode Line configuration mode

Usage Guide This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service cannot operate properly.

Configuration Examples The following example sets the hot key that disconnects the terminal service connection on line VTY 0 5 to **Ctrl+E** (0x05).

```
Hostname(config)# line vty 0 5
Hostname(config-line)# disconnect-character 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.12 escape-character

Use this command to set the escape character for the line. Use the **no** form of this command to restore the default setting.

escape-character *escape-value*

no escape-character

Parameter Description

Parameter	Description
escape-value	Sets the ASCII value corresponding to the escape character for the

	line, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^** (**Ctrl+Shift+6**) and the ASCII decimal value is 30.

Command Mode Line configuration mode

Usage Guide After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

Configuration Examples The following example sets the escape character for the line to 23 (**Ctrl+w**).

```
Hostname(config)# line vty 0
Hostname(config-line)# escape-character 23
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.13 exec

Use this command to enable the line to enter the command line interface. Use the **no** form of this command to disable the function.

exec

no exec

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Line configuration mode

Usage Guide The **no exec** command is used to ban the line from entering the command line interface. You have to enter the command line interface through other lines,

Configuration Examples The following example bans line VTY 1 from entering the command line interface.

```
Hostname(config)# line vty 1
Hostname(config-line)# no exec
Hostname# show users
```

```
Line           User       Host(s)            Idle      Location
---------------- ------------ -------------------- ----------
   ------------------
*  0 con 0      ---        idle              00:00:00   ---
   1 vty 0      ---        idle              00:01:03   20.1.1.2
   3 vty 2       ---         idle                00:00:13   20.1.1.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.14 exec-character-bits

Use this command to configure the coded character set for the async line. Use the **no** form of this command to restore the default setting.

exec-character-bits { **7 | 8** }

no exec-character-bits

Parameter Description

Parameter	Description
7	Configures a 7-bit coded character set.
8	Configures an 8-bit coded character set.

Defaults The default is 8.

Command Mode LINE configuration mode

Usage Guide If you want to enter Chinese characters in the command line or display Chinese characters, graphs or other international characters, configure the **exec-character-bits 8** command.

Configuration Examples The following example configures a 7-bit coded character set for the async line.

```
Hostname(config)# line console 0
Hostname(config-line)#exec-character-bits 7
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 flowcontrol

Use this command to configure the flow control mode for the async line. Use the **no** form of this command to restore the default setting.

flowcontrol { **hardware | none | software** }

no flowcontrol { **hardware | none | software** }

Parameter Description

Parameter	Description
hardware	Configures hardware flow control.
none	Configures no flow control.
software	Configures software flow control.

Defaults No flow control is configured by default.

Command Mode LINE configuration mode

Usage Guide This command is used to control the data sending rate to make it consistent with the receiving rate at the receiving end. The terminal cannot receive data while sending data, so this function prevent s data drop. Flow control is also configured for the communication between high speed device and low speed device (for example, printer and network interface). The system provides two flow control modes, namely, software flow control and hardware flow control. The stop and start characters are Ctrl+S (XOFF, ASCII: 19) and Ctrl+Q (XON, ASCII: 17) respectively.

Configuration Examples The following example configures software flow control for the async line.

```
Hostname(config)#line console 0
Hostname(config-line)#flowcontrol software
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.16 history

Use this command to enable command history for the line or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

history [**size** *size*]

no history

no history size

Parameter Description

Parameter	Description
size *size*	The number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the number of commands in the command history to 20 for line VTY 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)# history size 20
```

The following example disables the command history for line VTY 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)# no history
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 ipv6 access-class

Use this command to configure access to the terminal through IPv6 ACL. Use the **no** form of this command to restore the default setting.

ipv6 access-class *access-list-name* { **in** | **out** }

no ipv6 access-class *access-list-name* { **in** | **out** }

Parameter Description

Parameter	Description
access-list-name	Specifies the ACL name.
in	Filters the incoming connections.
out	Filters the outgoing connections.

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example uses the ACL named “test” to filter the outgoing IPv6 connections in line VTY 0 4.

```
Hostname(config)# line vty 0 4
Hostname(config-line)ipv6 access-list test out
```

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.18 length

Use this command to set the screen length for the line. Use the **no** form of this command to restore the default setting.

length *screen-length*

no length

Parameter Description

Parameter	Description
screen-length	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the screen length to 10.

```
Hostname(config-line)# length 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.19 line

Use this command to enter the specified LINE mode.

line [**console** | **vty**] *first-line* [*last-line*]

Parameter Description

Parameter	Description
console	Console port
vty	Virtual terminal line, applicable for telnet/ssh connection.
first-line	Number of first-line to enter
last-line	Number of last-line to enter

Defaults N/A

Command Mode Global configuration mode

Usage Guide

Configuration Examples The following example enters the LINE mode from LINE VTY 1 to 3:

```
Hostname(config)# line vty 1 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.20 line vty

Use this command to increase the number of VTY connections currently available. Use the **no** form of this command to restore the default setting.

line vty *line-number*

no line vty *line-number*

Parameter Description

Parameter	Description
line-number	Number of VTY connections, in the range from 0 to 35.

Defaults

Command Global configuration mode.

Mode

Usage Guide

Configuration Examples The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19.

```
Hostname(config)# line vty 19
```

The following example decreases the number of available VTY connections to 10. The available VTY connections are numbered 0-9.

```
Hostname(config)# line vty 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.21 location

Use this command to configure the line location description. Use the **no** form of this command to restore the default setting.

location *location*

no location

Parameter Description

Parameter	Description
location	Line location description

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example describes the line location as Swtich's Line VTY 0.

```
Hostname(config)# line vty 0
Hostname(config-line)# location Swtich's Line Vty 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.22 monitor

Use this command to enable log display on the terminal. Use the **no** form of this command to restore the default setting,

monitor

no monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example enables log display on the terminal in VTY line 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)# monitor
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.23 parity

Use this command to configure the parity for the async line. Use the **no** form of this command to restore the default setting.

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

no parity

Parameter Description

Parameter	Description
even	Configures even parity,
none	Configures no parity.

odd	Configures odd parity,

Defaults No parity check is configured by default.

Command Mode LINE configuration mode

Usage Guide Parity is required in communication through some devices (such as async serial ports and console ports).

Configuration Examples The following example configures even parity for the async line.

```
Hostname(config)#line console 0
Hostname(config-line)#parity even
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 privilege level

Use this command to set the privilege level for the line. Use the **no** form of this command to restore the default setting.

privilege level *level*

no privilege level

Parameter Description

Parameter	Description
level	Privilege level, in the range from 0 to 15.

Defaults The default is 1.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the privilege level for the line VTY 0 4 to 14.

```
Hostname(config)# line vty 0 4
Hostname(config-line)privilege level 14
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

3.25 show history

Use this command to display the command history of the line.

show history

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the command history of the line.

```
Hostname# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 show line

Use this command to display line configuration.

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

Parameter Description

Parameter	Description
console	Displays configuration for the console line.
vty	Displays configuration for the virtual terminal line.
line-num	Displays the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays configuration for the console port.

```
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
```

Field	Description
CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.
Type	Terminal type, including CON, and VTY.
speed	Asynchronous speed.
Overruns	The number of overrun errors received by the flash.
Line 0	Terminal line number.
Location: ""	Line location configuration.
Type: "vt100"	Compatibility standard.
Special Chars	Special characters, including Escape, Disconnect, and Activation characters.
Timeouts	Timeout value; “never” indicates no timeout.
History	Whether to enable command history; the number of commands in the command history.
Total input	Data volume received from the drive.
Total output	Date volume sent to the drive.

Data overflow	Overflowing data volume.
stop rx interrupt	Data reception interruption times.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.27 show privilege

Use this command to display the privilege level of the line.

show privilege

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the privilege level of the line.

```
Hostname# show privilege
Current privilege level is 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.28 show users

Use this command to display the login user information.

show users [**all**]

Parameter

Parameter	Description

Description

all	Displays line user information, including users logging into the line and users not logging into the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about users logging into the line,

```
Hostname# show users
Line           User        Host(s)             Idle      Location
---------------- ------------ -------------------- ----------
   ------------------
  0 con 0      ---         idle              00:00:46   ---
  1 vty 0      ---         idle              00:00:29   20.1.1.2
*  2 vty 1      ---         idle              00:00:00   20.1.1.2
```

The following example displays all line user information,

```
Hostname(config)# show users all
Line           User        Host(s)             Idle      Location
---------------- ------------ -------------------- ----------
   ------------------
  0 con 0      ---         idle              00:00:49   ---
  1 vty 0      ---         idle              00:00:32   20.1.1.2
*  2 vty 1      ---         idle              00:00:00   20.1.1.2
  3 vty 2      ---                           00:00:00   ---
  4 vty 3      ---                           00:00:00   ---
  5 vty 4      ---                           00:00:00   ---
   6 vty 5       ---                                 00:00:00   ---
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.29 speed

Use this command to configure the baud rate for the specified line. Use the **no** form of this command to restore the default setting,

speed *baudrate*

no speed

Parameter Description

Parameter	Description
baudrate	Sets the baud rate, in the range from 9600 to 115200.

Defaults The default is 9600.

Command Mode LINE configuration mode

Usage Guide N/A

Configuration Examples The following example sets the baud rate to 115200,

```
Hostname(config-line)# speed 115200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.30 start-character

Use this command to
on the async line. Use the **no** form of this command to restore the default setting.
start-character *ascii-value*
no start-character

Parameter Description

Parameter	Description
ascii-value	Sets the ASCII value corresponding to the start character for software flow control on the async line, in the range from 0 to 255.

Defaults The default is Ctrl+Q (ASCII: 17).

Command Mode LINE configuration mode

Usage Guide The start character marks the start of the data transmission.

Configuration Examples The following example configures Ctrl+Y (ASCII: 25) for starting software flow control on the async line,

```
Hostname(config)#line console 0
Hostname(config-line)#start-character 25
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.31 stopbits

Use this command to configure the stopbit number for every character for the async line. Use the **no** form of this command to restore the default setting.

stopbits { **1 | 2** }

no stopbits

Parameter Description	Parameter	Description
	1	Configures 1 stopbit.
	2	Configures 2 stopbits.

Defaults The default is 2.

Command Mode LINE configuration mode

Usage Guide The stopbit is required in communication between the async line and the async device (such as the conventional numb terminals and modems).

Configuration Examples The following example sets the stopbit number of every character for the async line to 1.

```
Hostname(config)#line console 0
Hostname(config-line)#stopbits 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.32 stop-character

Use this command to configure the stop character for software flow control on the async line. Use the **no** form of this command to restore the default setting.

stop-character *ascii-value*

no stop-character

Parameter Description

Parameter	Description
ascii-value	Sets the ASCII value corresponding to the stop character for software flow control on the async line, in the range from 0 to 255.

Defaults The default is Ctrl+S (ASCII: 19).

Command Mode LINE configuration mode

Usage Guide The stop character marks the end of the data transmission.

Configuration Examples The following example configures Ctrl+Z (ASCII: 26) for stopping software flow control on the async line,

```
Hostname(config)#line console 0
Hostname(config-line)#stop-character 26
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.33 terminal databits

Use this command to configure the databit number of the character for the current terminal in flow communication mode. Use the **no** form of this command to restore the default setting.

terminal databits *bit*

terminal no databits

Parameter Description

Parameter	Description
bit	Configures the databit number of the character, in the range from 5 to 8.

Defaults The default is 8.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the databit number of every character for the current terminal in flow communication mode to 7.

```
Hostname#terminal databits 7
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.34 terminal escape-character

Use this command to set the escape character for the current terminal. Use the **no** form of this command to restore the default setting.

terminal escape-character *escape-value*

terminal no escape-character

Parameter Description

Parameter	Description
escape-value	Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^** (**Ctrl+Shift+6**) and the ASCII decimal value is 30.

Command Mode Privileged EXEC mode

Usage Guide After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

Configuration Examples The following example sets the escape character for the current terminal to 23 (**Ctrl+w**).

```
Hostname# terminal escape-character 23
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.35 terminal exec-character-bits

Use this command to configure the coded character set for the current terminal. Use the **no** form of this command to restore the default setting.

terminal exec-character-bits { **7 | 8** }

terminal no exec-character-bits

Parameter Description

Parameter	Description
7	Configures a 7-bit coded character set.
8	Configures an 8-bit coded character set.

Defaults The default is 8.

Command Mode Privileged EXEC mode

Usage Guide If you want to enter Chinese characters in the command line or display Chinese characters, graphs or other international characters, configure the **exec-character-bits 8** command.

Configuration Examples The following example configures a 7-bit coded character set for the current terminal.

```
Hostname#terminal exec-character-bits 7
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.36 terminal flowcontrol

Use this command to configure the flow control mode for the current terminal. Use the **no** form of this command to restore the default setting.

terminal flowcontrol { **hardware | none | software** }

terminal no flowcontrol { hardware | none | software }

Parameter Description

Parameter	Description

hardware	Configures hardware flow control.
none	Configures no flow control.
software	Configures software flow control.

Defaults The default flow control mode is **none**.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures software flow control for the current terminal.

```
Hostname#terminal flowcontrol software
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.37 terminal history

Use this command to enable command history for the current terminal or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

terminal history [**size** *size*]

terminal no history

terminal no history size

Parameter Description

Parameter	Description
size *size*	Sets the number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the number of commands in the command history to 20 for the current terminal.

```
Hostname# terminal history size 20
```

The following example disables the command history for the current terminal.

```
Hostname# terminal no history
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.38 terminal length

Use this command to set the screen length for the current terminal. Use the **no** form of this command to restore the default setting.

terminal length *screen-length*

terminal no length

Parameter Description

Parameter	Description
screen-length	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the screen length for the current terminal to 10.

```
Hostname# terminal length 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.39 terminal location

Use this command to configure location description for the current device. Use the **no** form of this command to restore the default setting.

terminal location *location*
terminal no location

Parameter Description

Parameter	Description
location	Configures location description of the current device.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures location description of the current device as “Swtich’s Line Vty 0”.

```
Hostname# terminal location Swtich’s Line Vty 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.40 terminal parity

Use this command to configure the parity for the current terminal. Use the **no** form of this command to restore the default setting.
terminal parity { **even | none | odd** }
terminal no parity

Parameter Description

Parameter	Description
even	Configures even parity,
none	Configures no parity.
odd	Configures odd parity,

Defaults No parity check is configured by default.

Command Mode Privileged EXEC mode

Usage Guide Parity is required in communication through some devices (such as async serial ports and console ports).

Configuration Examples The following example configures even parity for the current terminal.

```
Hostname#terminal parity even
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.41 terminal speed

Use this command to configure the baud rate for the current terminal. Use the **no** form of this command to restore the default setting,

terminal speed *baudrate*

terminal no speed

Parameter Description

Parameter	Description
baudrate	Sets the baud rate, in the range from 9600 to 115200.

Defaults The default is 9600.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the baud rate for the current terminal to 115200,

```
Hostname# terminal speed 115200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.42 terminal start-character

Use this command to configure the start character for software flow control on the current terminal. Use the **no** form of this command to restore the default setting.

terminal start-character *ascii-value*
terminal no start-character

Parameter Description

Parameter	Description
ascii-value	Sets the ASCII value corresponding to the start character for software flow control on the current terminal, in the range from 0 to 255.

Defaults The default is Ctrl+Q (ASCII: 17).

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures Ctrl+Y (ASCII: 25) for starting software flow control on the current device,

```
Hostname#terminal start-character 25
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.43 terminal stopbits

Use this command to set the stopbit number of every character for the current terminal. Use the **no** form of this command to restore the default setting.
terminal stopbits { **1 | 2** }
terminal no stopbits

Parameter Description

Parameter	Description
1	Configures 1 stopbit,
2	Configures 2 stopbits.

Defaults The default is 2.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures 1 stopbit for the current terminal.

```
Hostname#terminal stopbits 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.44 terminal stop-character

Use this command to configure the stop character for software flow control on the current terminal.

Use the **no** form of this command to restore the default setting.

terminal stop-character *ascii-value*

terminal no stop-character

Parameter Description

Parameter	Description
ascii-value	Sets the ASCII value corresponding to the stop character for software flow control on the current terminal, in the range from 0 to 255.

Defaults The default is Ctrl+S (ASCII: 19).

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures Ctrl+Z (ASCII: 26) for stopping software flow control on the current device.

```
Hostname#terminal stop-character 26
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.45 terminal terminal-type

Use this command to configure the simulated terminal type string for the current terminal. Use the **no** form of this command to restore the default setting.

terminal terminal-type *terminal-type-string*

terminal no terminal-type

Parameter Description

Parameter	Description
terminal-type-string	Sets the terminal type string, such as vt100 and ansi.

Defaults The default is vt100.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the simulated terminal type string for the current terminal to ansi.

```
Hostname#terminal terminal-type ansi
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.46 terminal width

Use this command to set the screen width for the terminal.

terminal width *screen-width*

terminal no width

Parameter Description

Parameter	Description
screen-width	Sets the screen width for the terminal, in the range from 0 to 256.

Defaults The default is 79.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the screen width for the terminal to 10.

```
Hostname# terminal width 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.47 terminal-type

Use this command to configure the simulated terminal type string of the async line.

terminal-type *terminal-type-string*

no terminal-type

Parameter Description

Parameter	Description
terminal-type-string	Configures the terminal type string, such as vt100 and ansi.

Defaults The default is vt100.

Command Mode LINE configuration mode

Usage Guide You can use the **terminal-type vt100** command to restore the default terminal type. If you want to enable telnet connection, you should use the simulated terminal type to perform terminal type negotiation (Telnet: 0x18). See RFC 854 for details.

Configuration Examples The following example sets the simulated terminal type of the async line to ansi.

```
Hostname(config)#line console 0
Hostname(config-line)#terminal-type ansi
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.48 timeout login

Use this command to set the login authentication timeout for the line. Use the **no** form of this command to restore the default setting.

timeout login response *seconds*

no timeout login response

Parameter Description

Parameter	Description
response	The time period during which the line waits for the user to enter any message.
seconds	Timeout value, in the range from 1 to 300 in the unit of seconds.

Defaults The default is 30.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the login authentication timeout to 300 seconds for line VTY 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)login timeout response 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.49 transport input

Use this command to set the specified protocol under Line that can be used for communication. Use the **no** form of this command to restore the default setting.

transport input { **all** | **ssh** | **telnet | none** }

no transport input { **all** | **ssh** | **telnet** | **none** }

Parameter Description

Parameter	Description
all	Allows all the protocols under Line to be used for communication
ssh	Allows only the SSH protocol under Line to be used for communication

telnet	Allows only the Telnet protocol under Line to be used for communication
none	Allows none of protocols under Line to be used for communication

Defaults **all**, **ssh** and **telnet** protocols are allowed.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example specifies that only the Telnet protocol is allowed to login in line vty 0 4.

```
Hostname(config)# line vty 0 5
Hostname(config-line)transport input ssh
```

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.50 vacant-message

Use this command to set the logout message. Use the **no** form of this command to restore the default setting.

vacant-message [*c message c*]

no vacant-message

Parameter Description

Parameter	Description
c	Delimiter of the logout message, which is not allowed within the message.
message	Logout message.

Defaults N/A

Command Mode Line configuration mode

Usage Guide This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly, The logout message is displayed when the user logs out.

Configuration The following example sets the logout message to “Logout from the device”.

Examples

```
Hostname(config-line)#vacant-message @ Logout from the device @
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.51 width

Use this command to set the screen width for the line. Use the **no** form of this command to restore the default setting,

width *screen-width*

no width

Parameter Description

Parameter	Description
screen-width	Sets the screen width for the line, in the range from 0 to 256,

Defaults The default is 79.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the screen width for the line to 10.

```
Hostname(config-line)# width 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4 File System Commands

4.1 cd

Use this command to set the present directory for the file system.

cd *[filesystem:] [directory]*

Parameter Description

Parameter	Description
filesystem:	The URL of filesystem, followed by a colon (:). The filesystem includes **flash:**, **usb:**, and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

Defaults The default directory is the flash root directory.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples

Related Commands

Command	Description
pwd	Displays the present word directory.

Platform Description N/A.

4.2 copy

Use this command to copy a file from the specified source directory to the specified destination directory.

copy *source-url destination-url*

Parameter Description

Parameter	Description
source-url	Source file URL, which can be local or remote.
destination-url	Destination file URL, which can be local or remote.

Defaults N/A.

Command Privileged EXEC mode.

Mode

Usage Guide when the file to be copied exists on the target URL, the target file system determines the action, such as error report, overwrite, or offering you the choice.

The following table lists the URL:

Prefix	Description
running-config	Running configuration file.
startup-config	startup configuration file.
flash:	local FLASH file system.
tftp:	The URL of TFTP network server, in the format as follows: **tftp**:[[//location]/directory]**/filename**
oob_tftp:	The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.

Configuration Examples The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfile file exists locally.

```
 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.
```

Related Commands

Command	Description
delete	Deletes the file.
rename	Renames the file.
dir	Displays the file list of the specified directory.

Platform Description N/A

4.3 delete

Use this command to delete the files in the present directory.

delete { [*filesystem***:**] *file-url* | **startup-config** }

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
startup-config	The startup configuration file.

Defaults The default *filesystem*: is **flash:**.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples The following example deletes the fstab file on the FLASH disk.

```
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)

Related Commands

Command	Description
copy	Copies the file.
dir	Displays the file list of the specified directory.

Platform Description N/A

4.4 dir

Use this command to display the files in the present directory.

dir [*filesystem*:] [*directory*]

Parameter Description

Parameter	Description
filesystem	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a

	relative path.

Defaults By default, only the information under the present working path is displayed.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples The following example displays the file information of the root directory in the FLASH disk.

```
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)
```

Field	Description
1, 2, 3	Index number
-rw-	Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

Related Commands

Command	Description
pwd	Displays the present directory.
cd	Sets the present directory of the file system.

Platform Description N/A.

4.5 erase

Use this command to erase the device or file that does't have a file system.

erase *filesystem*

Parameter Description

Parameter	Description
filesystem:	Name of the file system, followed by a colon (:). For example, usb0:.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example erases the USB filesystem.

```
Hostname#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 …
Erase disk usb0 done!
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 file

Use this command to display the information about a file.

file [*filesystem*:] *file-url*

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
file-url	The file name containing the path. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem*: is **flash:**.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about gcc executable file.

```
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
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.7 file prompt

Use this command to set the prompt mode.

file prompt [**noisy** | **quiet**]

Parameter Description	Parameter	Description
	noisy	Displays prompt for all operation.
	quiet	Displays prompt rarely.

Defaults The default mode is noisy.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the prompt mode to noisy.

```
Hostname#file prompt noisy
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.8 mkdir

Use this command to create a directory.

mkdir [*filesystem*:] *directory*

Parameter Description	Parameter	Description
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
	directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem*: is **flash**:.
The default *directory* is the root directory.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples The following example creates a directory named 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)
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)
```

Related Commands

Command	Description
rmdir	Deletes the directory.
pwd	Displays the present directory.

Platform Description N/A

4.9 more

Use this command to display the content of a file.

more [/**ascii** | /**binary**] [*filesystem*:] *file-url*

Parameter Description

Parameter	Description
/**ascii**	Displays the file content in the ASCII format.
/**binary**	Displays the file content in the
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.

file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The file is displayed in its own format by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the content of the netconfig file under root directory of FLASH disk.

```
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    -      -
tcp       tpi_cots_ord  v    inet    tcp    -      -
udp6      tpi_clts     v    inet6   udp    -      -
tcp6      tpi_cots_ord  v    inet6   tcp    -      -
rawip     tpi_raw      -    inet     -     -      -
local     tpi_cots_ord  -    loopback  -     -      -
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.10 pwd

Use this command to display the working path.

pwd

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Usage Guide

Configuration Examples

Related Commands

Command	Description
cd	Changes the file system in the present directory.

Platform Description N/A.

4.11 rename

Use this command to move or rename the specified file.

rename *src-url dst-url*

Parameter Description

Parameter	Description
src-url	The source file URL to move.
dst-url	The URL of the destination file or directory.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example renames the fstab file in the root directory on the FLASH disk as new-fstab.

```
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)
```

Related Commands	Command	Description
	delete	Deletes the file.
	copy	Copies the file.

Platform Description N/A

4.12 rmdir

Use this command to delete an empty directory.

rmdir [*filesystem*:] *directory*

Parameter Description	Parameter	Description
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
	directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem*: is **flash:**.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples The following example deletes the null test directories.

```
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)
```

Related Commands	Command	Description
	N/A.	N/A.

Platform Description N/A.

4.13 show disk

Use this command to display USB/Flash information.

show disk *usb*/*flash*

Parameter Description	Parameter	Description
	usb	Displays USB information.
	flash	Displays FLASH information.

Defaults N/A

Command Mode User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays Flash information.

```
Hostname#show disk flash
Nand flash size: 512MB
Nor flash size: 1MB
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.14 show file systems

Use this command to display the file system information.

show file systems

Parameter Description	Parameter	Description
	N/A.	N/A.

Defaults N/A.

Command Mode User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples The following example displays the file system information:

```
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:
       NA           NA    xmodem    rw  xmodem:
     8192         2416     disk    rw  flash:
  1048576       548576     disk    rw  usb0:
```

Field	Description
Size(KB)	File system space, in the unit of KB.
Free(KB)	Available file system space, in the unit of KB.
Type	File system type
Flags	Permissions on the file system include: ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

Related Commands	Command	Description
	N/A.	N/A.

Platform Description N/A.

4.15 show mount

Use this command to display the mounted information.

show mount

Parameter	Parameter	Description

Description	N/A	N/A

Defaults N/A

Command Mode User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the mounted information.

```
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)
```

Field	Description
proc	Source address of mount.
on	-
/proc	Destination address of mount.
type	-
proc	Mount type.
(rw,noexec,nosuid,nodev)	Mount property.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.16 tree

Use this command to display the file tree of the current directory.

tree [*filesystem*:] [*directory*]

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem*: is **flash:**.

Command Mode User EXEC mode/Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the file tree of flash:/echo

```
Hostname#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
¦   +-- echo.o
¦   +-- echo_server.c
¦   +-- echo_server.o
¦   +-- echo_sysfs.c
¦   +-- echo_sysfs.h
¦   +-- echo_sysfs.o
¦   +-- Makefile
¦   +-- modules.order
```

```
¦   +-- Module.symvers
¦   +-- msg_fd.c
¦   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_os.ko
+-- user_space
   +-- echo_server.c
   +-- echo_server.o
   +-- Makefile
   +-- msg_fd.c
   +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.17 verify

Use this command to compute, display and verify Message Digest 5 (MD5).

verify [**/md5** *md5-value*] *filesystem***:** [*file-url*]

Parameter Description	Parameter	Description
	/md5	Computes and displays MD5.
	md5-value	The file MD5, which is compared with the computed MD5.
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:** and **tmp:**.
	file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem:* is **flash:**.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example computes MD5 of flash:/gcc.

```
Hostname#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

The following example computes MD5 and makes a comparison.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5 SYS Commands

5.1 calendar set

Use this command to set the hardware calendar.

calendar set { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [:minute [:second]]	Sets hardware time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can be reset. The unspecified parameters keep the current system values.
month	Sets month. The range is from 1 to 12.
day	Sets date. The range is from 1 to 31.
year	Sets year. The range is from 1970 to 2037.

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide

1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value. For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **calendar set** *12 5* command to change the current time into "2012-05-29 12:33:44".

The hardware time of the system is used as the UTC time, while the software time of the system refers to the local time of the device.

Configuration Examples The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.

```
Hostname# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
Hostname# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Hostname# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

Because the *hour* parameter is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

Check Method -

Platform Description -

5.2 clock read-calendar

Use this command to enable the system to synchronize the software time with the hardware time.

clock read-calendar

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide After you configure this command, the system will synchronize the software time with the current hardware time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the software time with the hardware time.

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

Check Method -

Platform Description -

5.3 clock set

Use this command to set the system software clock.

clock set { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [:minute [:second]]	Sets software time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can reset. The unspecified parameters keep the current system values.
month	Sets month. The range is from 1 to 12.
day	Sets date. The range is from 1 to 31.
year	Sets year. The range is from 1970 to 2037.

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide

1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value.

For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **clock set** *12 5* command to change the current time into "2012-05-29 12:33:44".

Configuration Examples The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.

```
Hostname# clock set 6
06:48:13 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
Hostname# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Hostname# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

Because the *hour* parameter in this command is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

Check Method -

Platform Description -

5.4 clock summer-time

Use this command to set the summer time.

clock 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*]

Use this command to disable the summer time.

no clock summer-time

Parameter Description

Parameter	Description
zone	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
start	Indicates the start time of the summer time.
start-month	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
week	Start week in the start month. The range is from 1 to 5.
last	The last week of the specified month.
start-date	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
hh:mm	Time, in the format of hour : minute.
end	Indicates the end time of the summer time.
end-month	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
ahead	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
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* has been set to 0, you are not allowed to set *minutes-offset* to 0.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide

Configuration Examples If the time zone name is ABC and the standard time is 8:15 ahead of UTC, namely, GMT+08:15. The summer time period starts from the first Saturday in February to the third Monday in May and the summer time is 01:20 ahead of the standard time. In this case, the summer time is 09:35 ahead of the UTC time,

but non-summer time is still 08:15 ahead of the UTC time.

```
Hostname(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
Hostname(config)#show clock
16:39:16 ABC Wed, Feb 29, 2012
Hostname(config)#show calendar
08:24:35 GMT Wed, Feb 29, 2012

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-5-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# show clock
18:00:08 TZA Wed, Feb 29, 2012

# If the time is set to non-summer time, the time zone name is restored to ABC.
Hostname#clo set 18 1 1
*Jan  1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
Hostname#show clock
18:00:12 ABC Sun, Jan  1, 2012
```

If the system uses the default summer time that is one hour ahead of the standard time, ahead and the parameters behind ahead can be neglected. For example, set the summer time to start from 2:00 a.m. of the first Sunday in April to 2:00 a.m. of the last Sunday in October and set the summer time to one hour ahead of the standard time.

```
Hostname(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO
October the last Sunday at 2:00, ahead 1 hour
Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead
1 hour
```

The following example disables summer time.

```
Hostname(config)#no clock summer-time
*Jan  1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

Check Method -

Platform Description -

5.5 clock timezone

Use this command to set the time zone.

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

Use this command to remove the time zone settings.

no clock timezone

Parameter Description

Parameter	Description
name	Time zone name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The name contains 3 to 31 characters.
hours-offset	Hours of time difference. It indicates whether the time is faster or smaller than the hardware UTC time. The range is from -12 to 12. The negative digit indicates that the time is slower than the hardware time, while the positive digit indicates that the time is faster than the hardware time. If the time is slower than the UTC time, add "-" before *hours-offset*.
minutes-offset	Minutes of time difference. The range is from 0 to 59.

Defaults

-

Command Mode

Global configuration mode

Default Level

-

Usage Guide

Configuration Examples

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

```
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
```

The following example sets the time zone name TZA. The software time is 06:13 slower than the hardware time.

```
Hostname(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)
```

The following example removes the time zone settings.

```
Hostname(config)# no clock timezone
```

```
Set no clock timezone.
```

Check Method -

Platform Description -

5.6 clock update-calendar

Use this command to enable the system to synchronize the hardware time with the software time.

clock update-calendar

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide After you configure this command, the system will synchronize the hardware time with the current software time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the hardware time with the software time.

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

The following example sets the time zone of the hardware time to GMT+5:10, which indicates that the hardware time is 5:10 slower than the software time. The summer time is not set.

```
Hostname# show clock
09:30:21 TSZ Wed, Feb 29, 2012

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

Hostname#show calendar
04:20:25 UTC Wed, Feb 29, 2012
```

The following example sets the hardware time. If it is set to GMT+5:10 and the summer time is set to be 1:15 faster from the first Monday in February 1 to the second Sunday in June 1, it indicates that the hardware time is 6:25 slower than the software time during the effective period of the summer time.

```
Hostname# show clock
09:30:02 TSZ Wed, Feb 29, 2012

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

Hostname#show calendar
03:05:08 UTC Wed, Feb 29, 2012
```

Check Method -

Platform Description -

5.7 cpu high-watermark set

Use this command to set the high and low watermark of the CPU usage of the control core and enable CPU usage monitoring.
cpu high-watermark set [[**up** *up-value*] [**down** *down-value*]]

Use this command to disable CPU usage monitoring.
no cpu high-watermark set

Use this command to restore the default settings.
default cpu high-watermark set

Parameter Description

Parameter	Description
high *high***up** *up-value*	Sets the high watermark of the CPU usage. The range is from 1 to 99.
range *range***down** *down-value*	Sets the low watermark of the CPU usage. The range is from 1 to 99.

Defaults By default, the high watermark is 85% and the low watermark is 75%.

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in vsd0.
You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.

Configuration Examples The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).

```
Hostname(config)# default cpu high-watermark set
Reset default cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

The following example disables CPU usage monitoring.

```
Hostname(config)# no cpu high-watermark set
Close cpu watermark monitor
```

The following example enables CPU usage monitoring. Keep the defined watermark value.

```
Hostname(config)# cpu high-watermark set
Open cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

The following example enables CPU usage monitoring and sets the high watermark to 90% and the low watermark to 70%.

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

In this case, the high watermark is 90% and the low watermark is 70%.

Check Method -

Prompt Message If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:

```
*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high
```

```
watermark(91%),current cpu usage 100%
```

When the CPU usage is less than the lower limit of the high watermark, the system will print the following message about warning release:

```
*Jan 20 07:02:52:  %RG_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%
```

Platform Description -

5.8 memory history clear

Use this command to clear the history of the memory usage.

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

Parameter Description

Parameter	Description
one-forth	Clears one fourth entries.
half	Clears a half of entries.
all	Clears all the entries.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example clears a half of the history of the memory usage.

```
Hostname# show memory history

Time Thu Jan  1 00:24:45 1970
Used(k) 148516
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      60600
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
Process Name    Holding
```

```
tcpip.elf       270028
cli-memory      52408
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148444
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      44088
rg_syslogd      36640

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

Check Method -

Prompt Message -

Platform Description -

5.9 memory low-watermark set

Use this command to set the low watermark threshold of the memory and enable the memory low watermark detection.
memory low-watermark set *mem-value*

Use the **no** or **default** form of this command to disable the detection of memory low watermark.
no memory low-watermark set

Parameter Description

Parameter	Description
mem-value	Memory watermark threshold. The range is from 1 KB to 4,294,967,295 KB.

Defaults By default, the detection of memory low watermark is disabled.

Command Mode Global configuration mode

Default Level -

Usage Guide You can use this command to enable the detection of the memory low watermark and set the memory watermark threshold. When the system memory is less than this threshold, the system will print prompts.

Configuration Examples The following example sets the low watermark threshold of the memory to 500,000 KB and enables detection.

```
Hostname(config)#memory low-watermark 500000
```

Check Method -

Prompt Message

Platform Description -

5.10 reload

Use this command to reload the device.

reload [**at** { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [:*minute* [:*second*]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
month	Sets the month, in the range from 1 to 12.
day	Sets the day, in the range from 1 to 31.
year	Sets the year, in the range from 1970 to 2069.

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide -

Configuration Examples The following example reloads the device.

```
Hostname# reload
Reload system?(Y/N) Y
Sending all processes the TERM signal...                    [  OK  ]
Sending all processes the KILL signal...                    [  OK  ]
Restarting system...
```

Check Method -

Prompt Message -

Platform Description -

5.11 show calendar

Use this command to display the hardware calendar.

show calendar

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the hardware calendar.

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

Prompt Message -

Platform Description -

5.12 show clock

Use this command to display the system software clock.

show clock

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode / global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the software clock when the time zone is disabled.

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

The following example displays the software clock when the time zone is enabled.

```
Hostname# show clock
03:07:49 TSZ Wed, Feb 29, 2012
```

Prompt Message -

Platform Description -

5.13 show cpu

Use this command to display the information on the system task running on the control core instead of the non-virtual core.

show cpu

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide If the system is equipped with a virtual core, you can use the **show processes cpu** command to check the CPU usage of the virtual core.

Configuration Examples The following example displays the information on the system task running on the control core instead of the non-virtual core.

```
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--
```

Prompt Message -

Platform Description -

5.14 show memory

Use this command to display the system memory.

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

Parameter Description

Parameter	Description
sorted total	Ranked according to the memory usage.
history	Displays the history of memory usage.
low-watermark	Displays the memory low watermark threshold of the system.
process-id	Displays the memory usage of the task specified by *process-id*.
process-name	Displays the memory usage of the task specified by *process-name*.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide Every time when the **show memory history** command is used, the number of displayed entries increases by one. Up to 10 entries can be displayed. You can use the **memory history clear** command to clear history entries.

Configuration Examples The following example displays the memory usage of each task and the ranking (based on the total memory usage).

```
Hostname# show memory sorted
System Memory: 508324K total, 160124K used, 348200K free, 31.5% used rate
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--
```

Description of some keywords in the command:

Keyword	Description
total	Total system memory
used	Used memory
free	Remaining memory
used rate	Memory usage (percentage)
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by Slab
others	Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.

Description of the displayed information on each task:

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

Prompt Message

-

Platform Description

-

5.15 show pci-bus

Use this command to display the information on the device mounted to the PCI bus.

show pci-bus

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the information on the device mounted to the PCI bus.

```
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
```

Prompt Message -

Platform Description -

5.16 show processes cpu

Use this command to display system task information.

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

Parameter Description

Parameter	Description
5sec | 1min | 5min | 15min	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
nonzero	Does not display the task with 0 CPU usage.
history	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
table	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide

Configuration Examples The following example displays the tasks listed in ascending order of task IDs.

```
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--
```

The following example displays the tasks listed in ascending order of task IDs without displaying the tasks

with 0 CPU usage within 15 minutes.

```
Hostname# show processes cpu nonzero
```

Description of the information displayed in this command:

Field	Description
System Uptime	Total running time of the device, precious to seconds.
CPU Utilization	Total CPU usage of the control core within the last five seconds, one minute, and five minutes.
Virtual CPU usage	Total CPU usage of the virtual control core within the last five seconds, one minute, and five minutes.
Tasks Statistics	Task statistics information, including the total number of statistics tasks and the task status.
set system cpu watermark	CPU watermark value and status of the control core.

The task running statuses are listed below:

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

Description of each task:

Field	Description
Pid	Task ID
S	Task status. Five statuses in total: R (running), T (stopped), S (sleeping), D (waiting), and Z (zombie).
PRI	Task running priority
P	The core of the CPU on which the task runs
5sec/1min/5min/15min	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores 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 in ascending order of task IDs and only the processes with non-zero CPU usage within 15 minutes are displayed.

```
Hostname #show processes cpu nonzero
```

The following example displays the CPU usage in descending order within five seconds and the tasks with zero CPU usage within one second are not displayed.

```
Hostname #show processes cpu 5sec nonzero
```

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

The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate nearest to 0 is the CPU usage in the last five seconds, measured in %.

The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

The third histogram displays the CPU usage of the control core within the last 72 hours, measured in %. Every segment on the x-coordinate is 1 hour.

Example:

```
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)
--------------------------------------------------------------------------------
```

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

The first table lists the CPU usage within 300 seconds. The first cell indicates the CPU usage within the last five seconds.

The second table lists the CPU usage within the last 60 minutes, measured in %. The two adjacent cells show the CPU usage measured at an interval of one minute.

The third table lists the CPU usage within the last 72 hours, measured in %. The two adjacent cells show the CPU usage measured at an interval of one hour.

Example:

```
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|
#-------------------------------------------------------------------------------#
```

Prompt Message -

Platform Description -

5.17 show processes cpu detailed

Use this command to display the details of the specified task.

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

Parameter Description

Parameter	Description
process-id	Displays the information on the task of the specified task ID.
process-name	Displays the information on the task of the specified task name.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide

Configuration Examples The following example displays the information on the task of the specified task name.

```
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     :
    Lass  5 sec     0.3% (0.6%)
    Lass  1 min     0.3% (0.6%)
    Lass  5 min     0.3% (0.6%)
    Lass 15 min     0.3% (0.6%)
Tty           : ?
```

Code Usage: 209.6 KB. If the specified task name is not unique, the system displays the following message:

```
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.
```

Description of the displayed information:

Field	Description
Process Id	Task ID
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 for the task from self-startup to now
Run Time	Duration for the task from self-startup to being executed
Cpu Usage	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the 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 "Primary device ID, secondary device ID". If it is 0, the value is **?**.
Code Usage	Size occupied by the task code segment

The following example displays the information on the task of the specified task ID.

```
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.
```

Prompt Message -

Platform Description -

5.18 show reboot-reason

Use this command to display the reboot reason.

show reboot-reason [*all*]

Parameter Description

Parameter	Description
all	Displays the reboot reason of all devices/service modules

Command Mode Privileged EXEC mode/ global configuration mode/ User EXEC mode

Default Level -

Usage Guide -

Configuration The following example displays the reboot reason of the device.

Examples

```
Hostname#show reboot-reason
time: 1970-01-01 08:03:13
reason: reload cmd
info: /sbin/rg-sysmon/3844

Hostname#
```

Prompt Message -

Platform Description -

5.19 show version

Use this command to display the system version information.

show version

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Usage Guide The following example displays the system version information.

```
Hostname# show version
System description     : Hostname Indoor AP320-I (802.11a/n and 802.11b/g/n)
System start time      : 2012-12-06 00:00:00
System uptime          : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number    : 1234942570018
System boot version     : 1.0.0
```

Prompt Message -

Platform Description -

6 Time Range Commands

6.1 absolute

Use this command to configure an absolute time range.
absolute { [**star**t *time date*] [**end** *time date*] }

Use the **no** form of this command to remove the absolute time range.
no absolute

Parameter Description

Parameter	Description
start *time date*	Indicates the start time of the range.
end *time date*	Indicates the end time of the range.

Defaults The default absolute time range is the maximum range.

Command Mode Time range configuration mode

Default Level 14

Usage Guide Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.
The maximum absolute time range is from 00:00 January 1, 0 to 23:59 December 31, 9999.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

The following example configures an absolute time range.

```
Hostname(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message -

Platform Description -

6.2 periodic

Use this command to configure periodic time.

periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

Use the **no** form of this command to remove the configured periodic time.

no periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

Parameter Description

Parameter	Description
day-of-the-week	Indicates the week day when the periodic time starts or ends.
time	Indicates the exact time when the periodic time starts or ends.

Defaults No periodic time is configured by default.

Command Mode Time range configuration mode

Default Level 14

Usage Guide Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time. If you want to modify the periodic time, it is recommended to disassociate the time range first and associate the time range after the periodic time is modified.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

The following example configures a periodic time interval.

```
Hostname(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message -

Platform Description -

6.3 show time-range

Use this command to display the time range configuration.

show time-range [*time-range-name*]

Parameter Description

Parameter	Description
time-range-name	Displays a specified time range.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to check the time range configuration.

Configuration Examples The following example displays the time range configuration.

```
Hostname# show time-range
time-range entry: test (inactive)
  absolute end 01:02 02 February 2012
```

Prompt Message -

Platform Description -

6.4 time-range

Use this command to create a time range and enter time range configuration mode.
time-range *time-range-name*

Use the **no** form of this command to remove the configured time range.
no time-range *time-range-name*

Parameter Description

Parameter	Description
time-range-name	Time range name

Defaults No time range is configured by default.

Command Mode Global configuration mode

Default Level 2

Usage Guide Some applications (such as ACL) may run based on time. For example, an ACL can be effective within

certain time ranges of a week. To this end, first you must configure a time range. After the time range is created, you can configure relevant time control in time range mode.

Configuration Examples

The following example creates a time range.

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

Check Method

Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message

-

Platform Description

-

7 HTTP Service Commands

7.1 enable service web-server

Use this command to enable the HTTP service function.

Use the **no** or **default** form of this command to disable the HTTP service function.

enable service web-server [**http** | **https** | **all**]

no enable service web-server [**http** | **https**]

default enable service web-server [**http** | **https**]

Parameter Description

Parameter	Description
http	Enables the HTTP service.
https	Enables the HTTPS service.
all	Enables both the HTTP service and the HTTPS service.

Defaults By default, the HTTP service function is disabled.

Command mode Global configuration mode.

Usage Guide If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

Configuration Examples The following example enables both the HTTP service and the HTTPS service:

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#enable service web-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

http port *port-number*

no http port

Parameter Description

Parameter	Description
port-number	Configures the HTTP port number. The value includes 80, 1025 to 65,535.

Defaults The default HTTP port number is 80.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP port number.

Configuration Examples The following example configures the HTTP port number as 8080:

```
Hostname(config)#http port 8080
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the default HTTPS port number.

http secure-port *port-number*

no http secure-port

Parameter Description

Parameter	Description
port-number	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.

Defaults The default HTTP port number is 443.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTPS port number.

Configuration Examples The following example configures the HTTPS port number as 4443:

```
Hostname(config)#http secure-port 4443
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.
show web-server status	Displays the configuration and status of the Web service.

Platform Description N/A

7.4 show web-server https certificate information

Use this command to display HTTPS certificate information.

show web-server https certificate information

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays HTTPS certificate information.

```
Hostname# show web-server https certificate information
Source: Default
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.5 show web-server status

Use this command to display the configuration and status of the Web service.

show web-server status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration and status of the Web service:

```
Hostname#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.
http port	Configures the HTTP port number.
http secure-port	Configures the HTTPS port number.

Platform Description N/A

7.6 upgrade web

Use this command to upgrade the Web package in local file system.

upgrade web *uri*

Parameter Description

Parameter	Description
uri	The storage path of the Web package.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Please use the **copy** command to copy the Web package into the file system before you use this command to upgrade the Web package.

Configuration Examples The following example copies a Web package into the file system and upgrades the package.

```
Hostname#copy tftp://192.168.23.24/web.upd flash:/web.upd
Hostname#upgrade web flash:/web.upd
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform Description N/A

7.7 upgrade web download

Use this command to download the Web package from the TFTP server and upgrade the package automatically.

upgrade web download tftp: *path*

Parameter Description

Parameter	Description
tftp: *path*	*path* indicates the storage path of the Web package on the TFTP server. **tftp** indicates the system downloads the Web package from the TFTP server through the physical port and upgrades the Web package automatically.

Defaults N/A

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example downloads a Web package from the TFTP server and upgrades the package automatically.

```
Hostname#upgrade web download tftp://192.168.23.24/web.upd
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform Description N/A

7.8 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

webmaster level *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }

no webmaster level *privilege-level* [**username** name]

Parameter Description

Parameter	Description
privilege-level	Configures the user privilege-level.
name	Username.
password	Password.
0 | **7**	Password type; 0 indicates plaintext, 7 indicates ciphertext.
encrypted-password	Password text.

Defaults By default, two users are configured.

1. User1 is configured with privilege level 1, username of admin and plaintext password of admin.
2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.

Command mode Global configuration mode.

Usage Guide When HTTP is enabled, users can log in to the Web interface only after being authenticated. Use this command to configure the username and password for Web login authentication.
Use the **no webmaster level** *privilege-level* command to delete all the usernames and passwords with a specified *privilege-level.*
Use the **no webmaster level** *privilege-level* **username** *name* command to delete the specified username and password.

Usernames and passwords come with three permission levels, each of which includes at most 10 usernames and passwords.

Configuration Examples The following example configures the username and password for Web login authentication,

```
Hostname(config)#webmaster level 0 username password admin
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform Description N/A

7.9 web-server http redirect-to-https

Use this command to configure HTTP redirection to HTTPS. Use the **no** form of this command to restore the default settings.
web-server http redirect-to-https
no web-server http redirect-to-https

Parameter Description

Parameter	Description
N/A	N/A

Defaults HTTP redirection to HTTPS is disabled by default.

Command mode Global configuration mode

Usage Guide

Run the **no web-server http redirect-to-https** or **default web-server http redirect-to-https** to

disable HTTP redirection.

Both HTTP and HTTPS must be enabled.

If the destination IP address is an NAPT address, HTTP redirection may fail. Please disable NAPT if you enable want to access the device by using the HTTP protocol. If you want to access the device by using the HTTPS protocol, please use the HTTPS protocol directly.

Configuration Examples The following example enables HTTP redirection to HTTPS.

```
Hostname(config)# web-server http redirect-to-https
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.10 web-server https certificate

Use this command to install the HTTPS certificate. Use the **no** form of this command to restore the default settings.

web-server https certificate { **pem** *cert-filename* **private-key** *key-filename* } | { **pfx** *cert-filename* } [**password** *password-text*]

no web-server https certificate

Parameter Description

Parameter	Description
pem	Imports certificate and key file in pem format.
pfx	Imports the certificate in pfx format.
cert-filename	Specifies the name of the certificate in flash:.
key-filename	Specifies the name of the key file in flash:.
password-text	Specifies the decryption password for the key file.

Defaults N/A

Command mode Global configuration mode

Usage Guide Run the **copy** command to place the certificate and the key file into the flash partition before installing the certificate. After installation, the certificate and the key file can be deleted.

Run the **no web-server https certificate** command to delete the HTTPS certificate. The auto-signed certificate will be used after the HTTPS certificate is deleted.

This command is not displayed in running-config.

After you install the HTTPS certificate, the browser may ask you to add trust before accessing Web management. It is recommended to close the browser and then open the Web management page.

Configuration Examples The following example installs the HTTS certificate.

```
Hostname#configure terminal
Hostname(config)# web-server https certificate pfx usercert.pfx password 123456
*Feb 28 14:38:37: %HTTPD-4-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.11 web-server https generate self-signed-certificate

Use this command to generate the HTTPS self-signed-certificate again.

web-server https generate self-signed-certificate

Parameter Description

Parameter	Description
N/A	N/A

Defaults The HTTPS self-signed-certificate is enabled by default.

Command mode Global configuration mode

Usage Guide This command is a communication command. After running the command, please enter the information required by auto-signed certificate or press Ctrl+C to abort the operation.

If you have already installed HTTPS certificate, the HTTPS certificate will be used preferentially. The HTTPS certificate will not be replaced by the auto-signed certificate.

This command is not displayed in running-config.

After you install the HTTPS certificate, the browser may ask you to add trust before accessing Web management. It is recommended to close the browser and then open the Web management page.

Configuration Examples The following example generates the HTTPS self-singed-certificate again.

```
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.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8 Syslog Commands

8. 1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

clear logging

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

Configuration Examples The following example clears the log packets from the memory buffer.

```
Hostname# clear logging
```

Related Commands

Command	Function
logging on	Turns on the log switch.
show logging	Displays the logs in the buffer.
logging buffered	Records the logs in the memory buffer.

Platform Description N/A

8.2 logging

Use this command to send the log message to the specified syslog server.

logging { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]

Use this command to delete the specified syslog server.

no logging { *ip-address*] | **ipv6** *ipv6-address* }

Use this command to restore the default port 514.

no logging { *ip-address* | **ipv6** *ipv6-address* } **udp- port**

Parameter Description

Parameter	Description

ip-address	Sets the IP address of the host receiving log messages.
ipv6-address	Sets the IPv6 address of the host receiving log messages.
udp-port *port*	Sets the port number of the host receiving log messages. The default is 514.

Defaults No log message is sent to syslog server by default.

Command Mode Global configuration mode

Usage Guide This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously,

Configuration Examples The following example configures a syslog server with IP address 202.101.11.1.

```
Hostname(config)# logging 202.101.11.1
```

The following example configures a syslog server with IP address 202.101.11.1 and port number 8099.

```
Hostname(config)# logging 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname(config)# logging ipv6 AAAA:BBBB::FFFF
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer. Use the **default** form of this command to restore the default setting.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Parameter Description

Parameter	Description
buffer-size	Size of the buffer is related to the specific device type: For the access switches, 4 K to 1 M Bytes.
level	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

Defaults The buffer size is related to the specific device type.
access switches: 128 K Bytes;
The log severity is 7.

Command Mode Global configuration mode

Usage Guide The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command in privileged user mode.
The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the **clear logging** command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server.
The log information is classified into the following 8 levels (Table 1):

Table-1

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level. When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.

⚠ After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficent availble continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

Configuration Examples The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

```
Hostname(config)# logging buffered 10000 6
```

Related

Command	Description

Commands		
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	clear logging	Clears the logs in the log buffer.

Platform Description N/A

8.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

logging console [*level*]

no logging console

Parameter Description	Parameter	Description
	level	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.

Defaults The default is debugging (7).

Command Mode Global configuration mode

Usage Guide When a log severity is set, the log messages at or below that severity will be displayed on the console.
The **show logging** command displays the related setting parameters and statistics of the log.

Configuration Examples The following example sets the severity of log that is allowed to be displayed on the console as 6:

```
Hostname(config)# logging console informational
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs and related log configuration parameters in the buffer.

Platform Description N/A

8.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

logging count

no logging count

Parameter Description

Parameter	Description
N/A	N/A

Defaults The log statistics function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command enables the log statistics function. The statistics begins when the function is enabled. If you run the **no logging count** command, the statistics function is disabled and the statistics data is deleted.

Configuration Examples The following example enables the log statistics function:

```
Hostname(config)# logging count
```

Related Commands

Command	Description
show logging count	Displays log information about modules of the system.
show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.6 logging facility

Use this command to configure the device value of the log information in global configuration mode. Use the **no** form of the command to restore the default setting.

logging facility *facility-type*

no logging facility

Parameter Description

Parameter	Description
facility-type	Syslog device value. For specific settings, refer to the usage guide.

Defaults The default is 23 if the RFC5424 format is enabled (Local7, local use).
The default is 16 if the RFC5424 format is disabled (Local0, local use).

Command Mode Global configuration mode

Usage Guide The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization messages
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization messages
11 (ftp)	FTP daemon
12 (ntp)	NTP subsystem
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

The default device value of system is 23 (local 7).

Configuration Examples The following example sets the device value of **Syslog** as **kernel**:

```
Hostname(config)# logging facility kern
```

Related

Command	Description

Commands		
	logging console	Sets the severity of logs that are allowed to be displayed on the console.

Platform Description N/A

8.7 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB or SD card. Use the **no** form of this command to restore the default setting,

logging file { **flash:***filename* } [*max-file-size*] [*level*]

no logging file

Parameter Description

Parameter	Description
flash	Saves the log file in expanded FLASH.
filename	Sets the file name. The file type is omitted, which is fixed as txt.
max-file-size	Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K,
level	Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details.

Defaults Log messages are not saved in expanded FLASH by default.

Command Mode Global configuration mode

Usage Guide You can save log messages in expanded FLASH if you don't want to transmit log messages on the network or there is no syslog server,

The log file cannot be configured with the suffix, which is fixed as txt.

If there is no expanded FLASH, the **logging file flash** command is hidden automatically and cannot be configured.

Keyword	Level	Description
Emergencies	0	Emergency case. The system fails to run.
Alerts	1	Problem that call for immediate solution.
Critical	2	Critical message.
Errors	3	Error message.
warnings	4	Alarm message.

Notifications	5	message that is normal but calls for attention.
informational	6	Descriptive message.
Debugging	7	Debugging message

Configuration Examples The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively.

```
Hostname(config)# logging file flash:syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.8 logging file numbers

Use this command to set the number of log files written into FLASH. Use the **no** form of this command to restore the default setting.

logging file numbers *numbers*

no logging file numbers

Parameter Description

Parameter	Description
numbers	Sets the number of log files written into FLASH, in the range from 2 to 32.

Defaults The default is 16.

Command Mode Global configuration mode

Usage Guide The system does not delete previously generated log files even if you change this configuration, Therefore, you need to delete the log files manually to save FLASH size (you can send log files to the server through TFTP before that). For example, 16 log files are generated by default before you want to change the number to 2. New logs are overwritten constantly in log files indexed 0 to 1. However, log files indexed from 2 to 16 remain. You can delete these log files manually as needed.

Configuration Examples The following example sets the number of log files written into FLASH to 8.

```
Hostname(config)# logging file numbers 8
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

8.9 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the **no** form of this command to restore the default setting.

logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

no logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter Description

Parameter	Description
all	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
buffer	Log messages destined to the log buffer are filtered, including log messages displayed by running the **show logging** command.
file	Log messages destined to the log file are filtered.
server	Log messages destined to the log server are filtered.
terminal	Log messages destined to the console and the VTY terminal (including Telnet and SSH).

Defaults Log messages destined to all directions are filtered by default.

Command Mode Global configuration mode

Usage Guide In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the **terminal** parameter.

Configuration Examples The following example filters log messages destined to the terminal (including the console and the VTY terminal).

```
Hostname(config)# logging filter direction terminal
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.10 logging filter rule

Use this command to configure the filter rule of the log message,
logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] }
Use this command to delete the “exact-match” filter rule.
no logging filter rule exact-match [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]
Use this command to delete the “single-match” filter rule.
no logging filter rule single-match [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*]

Parameter Description

Parameter	Description
exact-match	Exact-match filter rule. Fill in all the following three parameters.
single-match	Single-match filter rule. Fill in one of the following three parameters.
module *module-name*	Module name.
mnemonic *mnemonic-name*	Mnemonic name.
level *level*	Log level,

Defaults No filter rule is configured by default,

Command Mode Global configuration mode

Usage Guide If you want to filter a specific log message, use the “exact-match” filter rule and fill in all three parameters, namely, module name, mnemonic name and log level.
If you want to filter a specific kind of log messages, use the “single-match” filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level.
When configured with the same module name, mnemonic name or log level, the “single-match” filter rule has a higher priority than the “exact-match” filter rule,

Configuration Examples The following example configures the “exact-match” filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT.

```
Hostname(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

The following example configures the “single-match” filter rule with the parameter of module name SYS.

```
Hostname(config)# logging filter rule single-match module SYS
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.11 logging filter type

Use this command to configure the filter type of log messages. Use the **no** form of this command to restore the default setting.

logging filter type { **contains-only** | **filter-only** }

no logging filter type

Parameter Description

Parameter	Description
contains-only	The log message containing the key word of the filter rule is printed.
filter-only	The log message containing the key word of the filter rule is filtered.

Defaults The default filter type is filter-only.

Command Mode Global configuration mode

Usage Guide

1. When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the “filter-only” filter type to filter the log messages,
2. If you are concerned with certain log messages, use the “contains-only” filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

In real operation, the contains-only and the fitler-only filter types cannot be configured at the same time.

If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.

Configuration Examples The following example sets the filter type to contains-only.

```
Hostname(config)# logging filter type contains-only
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

logging flash flush

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

Configuration Examples The following example writes log messages in the system buffer into the flash file immediately.

```
Hostname(config)# logging flash flush
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the **no** form of this command to restore the default setting.

logging flash interval *seconds*

no logging flash interval

Parameter Description

Parameter	Description
interval *seconds*	The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds.

Defaults The default is 3600.

Command Mode Global configuration mode

Usage Guide This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the **no logging flash interval** command.

To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

Configuration Examples The following example sets the interval to write log messages into the flash file to 300 seconds.

```
Hostname(config)# logging flash interval 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.14 logging life-time

Use this command to configure the preservation duration of logs in expanded FLASH. Use the **no** form of this command to restore the default setting.

logging life-time level *level days*

no logging life-time level *level*

Parameter Description

Parameter	Description
level	Sets the log level, which can be either the level name or the level number.
days	Sets the preservation duration of logs.

Defaults No preservation duration is set by default.

Command Mode Global configuration mode

Usage Guide Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

Once log preservation based on time is enabled, log preservation based on file size is disabled

automatically. The log files are stored under the syslog/ directory of the expanded FLASH,

Configuration Examples The following example sets the preservation duration of logs whose level is 6 to 10 days.

```
Hostname(config)# logging life-time level 6 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.15 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the **no** form of this command to disable this function.

logging monitor [*level*]

no logging monitor

Parameter Description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.

Defaults The default is debugging (7).

Command Mode Global configuration mode

Usage Guide To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**.
The log level defined with "Logging monitor" is for all VTY windows.

Configuration Examples The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

```
Hostname(config)# logging monitor informational
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description N/A

8.16 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this fucntion.

logging on

no logging on

Parameter Description

Parameter	Description
N/A	N/A

Defaults Logs are allowed to be displayed on different devices.

Command Mode Global configuration mode

Usage Guide Log information can not only be shown in the Console window and VTY window, but also be recorded in different equipments such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

Configuration Examples The following example disables the log switch on the device.

```
Hostname(config)# no logging on
```

Related Commands

Command	Description
logging buffered	Records the logs to a memory buffer.
logging server	Sends logs to the Syslog server.
logging file flash:	Records logs on the expanded FLASH.
logging console	Allows the log level to be displayed on the console.
logging monitor	Allows the log level to be displayed on the VTY window (such as telnet window) .
logging trap	Sets the log level to be sent to the Syslog server.

Platform Description N/A

8.17 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the **no** form of this command to disable this function.

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** *severity*]

no logging rate-limit

Parameter Description

Parameter	Description
number	The number of logs that can be processed in a second in the range from 1 to 10000.
all	Sets rate limit to all the logs with severity level 0 to 7.
console	Sets the amount of logs that can be shown in the console in a second.
except	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
severity	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.

Defaults The log rate limit function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to control the syslog outpt to prevent the massive log output.

Configuration Examples The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

```
Hostname(config)#logging rate-limit all 10 except warnings
```

Related Commands

Command	Description
show logging count	Displays log information about modules of the system.
show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.18 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

logging server { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]

no logging server { *ip-address*| **ipv6** *ipv6-address* }

no logging server { *ip-address* | **ipv6** *ipv6-address* } **udp-port**

Parameter Description

Parameter	Description
ip-address	IP address of the host that receives log information.
ipv6-address	Specifies IPV6 address for the host receiving the logs.
udp-port *port*	Specifies the port number for the specified host (The default port number is 514).

Defaults No log is sent to any syslog server by default.

Command Mode Global configuration mode

Usage Guide This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

Configuration Examples The following example specifies a syslog server of the address 202.101.11.1:

```
Hostname(config)# logging server 202.101.11.1
```

The following example specifies an ipv6 address as AAAA:BBBB:FFFF:

```
Hostname(config)# logging server ipv6 AAAA:BBBB:FFFF
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays log messages and related log configuration parameters in the buffer.
logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description N/A

8.19 logging source interface

Use this command to configure the source interface of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source [**interface**] *interface-type interface-number*

no logging source [**interface**]

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Defaults No source interface is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

Configuration Examples The following example specifies loopback 0 as the source address of the syslog messages:

```
Hostname(config)# logging source interface loopback 0
```

Related Commands

Command	Description
logging server	Sends logs to the Syslog server.

Platform Description N/A

8.20 logging source ip | ipv6

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source {**ip** *ip-address* | **ipv6** *ipv6-address*}

no logging source { **ip | ipv6** }

Parameter Description

Parameter	Description
ip-address	Specifies the source IPV4 address sending the logs to IPV4 log server.
ipv6-address	Specifies the source IPV6 address sending the logs to IPV6 log server.

Defaults No source address is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.

Configuration Examples The following example specifies 192.168.1.1 as the source address of the syslog messages:

```
Hostname(config)# logging source ip 192.168.1.1
```

Related Commands

Command	Description
logging server	Sends the logs to the Syslog server.

Platform Description N/A

8.21 logging synchronous

Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the **no** form of this command to restore the default setting.

logging synchronous

no logging synchronous

Parameter Description

Parameter	Description
N/A	N/A

Defaults The synchronization function between user input and log output is disabled by default.

Command Mode Line configuration mode

Usage Guide This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

Configuration Examples

```
Hostname(config)#line console 0
Hostname(config-line)#logging synchronous
```

Print UP-DOWN logs on the port when keying in the command, the input command will be output

again:

```
Hostname# configure terminal
Oct  9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state
to down
Oct  9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet 0/1, changed state to DOWN
Hostname# configure terminal//----the input command by the user is output
again rather than being intererupted.
```

Related Commands

Command	Description
show running-config	Displays the configuration.

Platform Description N/A

8.22 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the **no** form of this command to prohibit sending log messages to the Syslog server.

logging trap [*level*]

no logging trap

Parameter Description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

Defaults The default is informational(6)

Command Mode Global configuration mode

Usage Guide To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.
The **show logging** command displays the configured related parameters and statistics of the log.

Configuration Examples The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

```
Hostname(config)# logging 202.101.11.22
Hostname(config)# logging trap informational
```

Related Commands

Command	Description
logging on	Turns on the log switch.
logging	Sends logs to the Syslog server.
show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description N/A

8.23 logging userinfo

Use this command to enable the logging function to record user log/exit. Use the **no** form of this command to restore the default setting.

logging userinfo

no logging userinfo

Parameter Description

Parameter	Description
N/A	N/A

Defaults Log message is printed recording user log/exit by default.

Command Mode Global configuration mode

Usage Guide This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

Configuration Examples The following example enables the logging function to record user log/exit.

```
Hostname(config)# logging user-info
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.24 logging userinfo command-log

Use this command to enable the logging function to record user operation. Use the **no** form of this

command to restore the default setting.

logging userinfo command-log

no logging userinfo command-log

Parameter Description

Parameter	Description
N/A	N/A

Defaults Log message is printed recording user operation by default.

Command Mode Global configuration mode

Usage Guide This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68)
command-log: logging server 192.168.23.68.
```

Configuration Examples The following example enables the logging function to record user operation.

```
Hostname(config)# logging user-info command-log
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.25 service log-format rfc5424

Use this command to enable the RFC5424 format. Use the **no** form of this command to restore the default setting.

service log-format rfc5424

no service log-format rfc5424

Parameter Description

Parameter	Description
N/A	N/A

Defaults The RFC3164 format is used by default.

Command Mode Global configuration mode

Usage Guide After the RFC5424 format is enabled, the service sequence-numbers, service sysname, **service timestamps**, **service private-syslog** and **service standard-syslog** commands become invalid and hidden.
After switching back to the RFC3164 format, the **logging delay-send**, **logging policy** and **logging statistic** commands become invalid and hidden.
After switching the log format, the results of running the **show logging** and **show logging config** commands change,

Configuration Examples The following example enables the RFC5424 format.

```
Hostname(config)# service log-format rfc5424
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.26 service private-syslog

Use this command to set the syslog format to the private syslog format. Use the **no** form of this command to restore the default setting.
service private-syslog
no service private-syslog

Parameter Description

Parameter	Description
N/A	N/A

Defaults The syslog is displayed in the default format.

Command Mode Global configuration mode

Usage Guide By default, the syslog is displayed in the format as follows:
*timestamp: %facility-severity-mnemonic: description
Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:
timestamp facility-severity-mnemonic: description
Here is an example:

```
May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console
```

The difference between the private syslog format and the default syslog format lies in the following marks:

The private syslog does not have "*" before the timestamp, ":" after the timestamp and "%" before the identifying string.

Configuration Examples The following example sets the private syslog format.

```
Hostname(config)# service private-syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.27 service sequence-numbers

Use this command to attach serial numbers into the logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sequence-numbers

no service sequence-numbers

Parameter Description

Parameter	Description
N/A	N/A

Defaults No serial number is contained in the logs by default.

Command Mode Global configuration mode

Usage Guide In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

Configuration Examples The following example adds serial numbers to the logs.

```
Hostname(config)# service sequence-numbers
```

Related Commands

Command	Description
logging on	Turns on the log switch.
service timestamps	Attaches timestamps to the logs.

Platform Description N/A

8.28 service standard-syslog

Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the **no** form of this command to restore the default setting.

service standard-syslog

no service standard-syslog

Parameter Description

Parameter	Description
N/A	N/A

Defaults The syslog is displayed in the default format.

Command Mode Global configuration mode

Usage Guide By default, the syslog is displayed in the format as follows:

*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp %facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
```

The difference between the standard syslog format and the default syslog format lies in the following marks:

The standard syslog does not have "*" before the timestamp and ":" after the timestamp.

Configuration Examples The following example sets the standard syslog format.

```
Hostname(config)# service standard-syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.29 service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sysname

no service sysname

Parameter Description

Parameter	Description
N/A	N/A

Defaults No system name is attached to logs by default.

Command Mode Global configuration mode

Usage Guide This command allows you to decide whether to add system name in the log information.

Configuration Examples The following example adds a system name in the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
Hostname #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname (config)#service sysname
Hostname (config)#end
Hostname #
Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console
```

Related Commands

Command	Function
show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.30 service timestamps

Use this command to attach timestamp into logs in global configuration mode. Use the **no** form of this command to remove the timestamp from the logs. Use the **default** form of this command to restore the default setting.

service timestamps [*message-type* [**uptime | datetime** [**msec** | **year**]]]

no service timestamps [*message-type*]

default service timestamps [*message-type*]

Parameter Description

Parameter	Description
message-type	The log type, including **Log** and **Debug**. The **log** type indicates the log information with severity levels of 0 to 6. The **debug** type indicates that with severity level 7.
uptime	Device start time in the format of *Day*Hour*Minute*Second,

	for example, 07:00:10:41.
datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

Defaults The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

Command Mode Global configuration mode

Usage Guide When the **uptime** option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the **datetime** option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

Configuration Examples The following example enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```
Hostname(config)# service timestamps debug datetime msec
Hostname(config)# service timestamps log datetime msec
Hostname(config)# end
Hostname(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console
by console
```

Related Commands

Command	Description
logging on	Turns on the log switch.
service sequence-numbers	Enables serial numbers of logs.

Platform Description N/A

8.31 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.

show logging

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the result of the **show logging** command with RFC5424 format disabled.

```
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-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to down.
015490: *Sep 19 02:46:26: Hostname %LINEPROTON/A5N/AUPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Hostname %LINKN/A3N/AUPDOWN: Interface FastEthernet
0/24, changed state to up.
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
```

Log information description:

Field	Description

Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```
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 test - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z test CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z test - 7 - - Please config the IP address
```

```
for capwap.
<132>1 2013-07-24T12:20:32.250265Z test CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<134>1 2013-07-24T12:29:33.410123Z test SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z test SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands

Command	Function
logging on	Turns on the log switch.
clear logging	Clears the log messages in the buffer.

Platform Description N/A

8.32 show logging config

Use this command to display log configuration and statistics.

show logging config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the outcome of running the **show logging config** command with RFC5424 disabled.

```
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
```

Field	Description
Syslog logging	Whether the logging function is enabled or disabled.
Console logging	The level and statistics of the log message printed on the console.
Monitor logging	The level and statistics of the log message printed on the VTY window.
Buffer logging	The level and statistics of the log message recorded in the memory buffer.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of debugging message.
Timestamp log messages	Timestamp format of log message.
Sequence-number log messages	Whether the sequence number function is enabled or disabled.
Sysname log messages	Adds the system name to the log message.
Count log messages	Log-counting function
Trap logging	The level and statistics of the log message sent to the syslog server.

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
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
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to output console and remove terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending way and statistics

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.33 show logging count

Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.

show logging count

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.
You can use the **show logging** command to check whether the log statistics function is enabled.

Configuration Examples The following example displays the result of the **show logging count** command:

```
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
```

Related Commands

Command	Function
logging count	Enables the log statistics function.
show logging	Displays basic configuration of log modules and log information in the buffer.
clear logging	Clears the logs in the buffer.

Platform Description N/A

8.34 show logging reverse

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.
show logging reverse

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

Configuration Examples The following command displays the result of the **show logging reverse** command with RFC5424 format disabled.

```
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-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to down.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages

Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

```
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 test SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z test SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z test CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z test - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z test CAPWAP 4 NO_IP_ADDR - No ip address for
capwap.
<135>1 2013-07-24T12:19:33.130290Z test - 7 - - Please config the
IP address for capwap.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics

Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.35 terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to restore the default setting.

terminal monitor

terminal no monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults Log information is not allowed to be displayed on the VTY window by default.

Command Mode Privileged EXEC mode

Usage Guide This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.

Configuration Examples The following example allows log information to be printed on the current VTY window:

```
Hostname# terminal monitor
```

Related Commands	Command	Description
	N/A	N/A

Platform Description	
	N/A

Command History	Version	Description
	N/A	N/A

9 Secuirty Log Commands

Command	Function
secuirty-log audit-enable	Enable the security log auditing function.
security-log data-store-items	Configure the local storage capacity for security logs.
security-log delete	Clear logs for all key operations.
security-log data-store-days	Configure the local storage time of security logs.
security-log auto-vacuum-time	Configure the handling time of aged security logs.
show security-log	Display all security logs.
show security-log detail	Display detailed security log information.
show security-log config	Display security log configurations.
show security-log statistics	Display security log statistics.
show security-log info	Display statistics during log processing.

9.1 securirty-log audit-enable

Use this command to enable the security log auditing function.

security-log audit-enable

Use this command to disable the security log auditing function.

no security-log audit-enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The security log auditing function is enabled by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide 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.

Configuration Examples The following example enables the security log auditing function.

```
Hostname# configure terminal
Hostname(config)# security-log audit-enable
Hostname(config)# end
```

Verification Run the **show running-config** command or the **show security-log config** command to display configuration status.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

9.2 security-log data-store-items

Use this command to configure the maximum storage capacity for security logs.

security-log data-store-items *num*

Parameter Description

Parameter	Description
num	Indicates the local storage capacity for security logs.

Defaults The default maximum value of storage capacity is 10,000.

Command Mode Global configuration mode

Default Level 15

Usage Guide If local storage space is insufficient, you can run this command to adjust the storage capacity for security logs.

Configuration Examples The following example sets the local storage capacity for security logs to 5000.

```
Hostname# configure terminal
Hostname(config)# security-log data-store-items 5000
Hostname(config)# end
```

Verification Run the **show running-config** command or the **show security-log config** command to display configuration status.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

9.3 security-log delete

Use this command to clear all logs for key operations.

security-log delete all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to clear all logs for key operations.

Configuration Examples The following example clear all logs for key operations.

```
Hostname# security-log delete all
```

Verification Run the **show security-log** command to display logs after deletion.

Prompt Messages N/A

Platform Description N/A

9.4 security-log data-store-days

Use this command to configure the local storage time of security logs.

security-log data-store-days *day*

Parameter Description

Parameter	Description
day	The local storage time of security logs, in days. The value range is from 1 to 65535 and the default value is 180.

Defaults The default local storage time of security logs is 180 days.

Command Mode Global configuration mode

Default Level 15

Usage Guide The security logs for key operations are stored in the local database for 180 days by default, and expired logs will be deleted. Run this command to modify the storage time.

Configuration Examples The following example sets the local storage time for security logs to 300 days.

```
Hostname# configure terminal
Hostname(config)# security-log data-store-days 300
Hostname(config)# end
```

Verification Run the **show running-config** command or the **show security-log config** command to display configuration status.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

9.5 security-log auto-vacuum-time

Use this command to configure the handling time of aged security logs.

security-log auto-vacuum-time *hh:mm:ss*

Parameter Description

Parameter	Description
hh:mm:ss	hour:minute:second. The default handling time is 03:00:00.

Defaults The default handling time of aged security logs is 03:00:00.

Command Mode Global configuration mode

Default Level 15

Usage Guide By default, the system checks whether any local logs have exceeded the storage time at 03:00:00 every day and clears expired logs.

Run this command to modify the time to check local logs.

Configuration Examples The following example sets the handling time of aged security logs to 05:05:00 every day.

```
Hostname# configure terminal
Hostname(config)# security-log auto-vacuum-time 05:05:00
Hostname(config)# end
```

Verification Run the **show running-config** command or the **show security-log config** command to display configuration status.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

9.6 show security-log

Use this command to display all security logs.

show security-log

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to display all security logs.

Configuration Examples The following example displays all security logs.

```
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
.....
```

Prompt Messages N/A

Platform Description N/A

9.7 show security-log detail

Use this command to display detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

show security-log detail { **all |** { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peerinfo** *peerinfo*] **{** [**order-by** [**time** | **log-type**] { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]] **}**

Use this command to export detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

show security-log detail export { **all |** { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peerinfo** *peerinfo*] **{** [**order-by** [**time** | **log-type**] { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]] **}**

Use this command to display the count of detailed security log information, which can be filtered by

time, log type, username, host name, and terminal information.

show security-log detail stat { **all |** { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peerinfo** *peerinfo*]

Parameter Description

Parameter	Description
yyyy mm dd	*yyyy* specifies the year; *mm* specifies the month; *dd* specifies the day.
hh:mm:ss	*hh* specifies the hour; *mm* specifies the minute; *ss* specifies the second.
log-type	Log types, including the following options: (1) **SEC_LOG** (security log events, SECURITY-LOG-EVENT); (2) **ACC_MNT** (account management, ACCOUNT-MANAGEMENT); (3) **LOGIN** (login events, LOGIN-EVENT); (4) **SYS** (system events, SYSTEM-EVENT); (5) **CONFIG** (configuration file changes, CONFIGURATION-CHANGES); (6) **OTHER** (others, OTHER)
username	A filter condition that matches the user name with security logs exactly.
hostname	A filter condition that matches the host name with security logs exactly.
peerinfo	A filter condition that match the terminal information with security logs through fuzzy matching. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).
integer1	The start position in the search result.
integer2	The end position in the search result.

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to display or export detailed security log information.

Configuration Examples The following example displays security logs of the user “user A” from 00:00 on October 10, 2019 to 24:00 on October 22, 2019, and sorts the logs in descending order of time. Only the first twenty records are displayed.

```
Hostname# show security-log detail from 2019 10 10 00:00:00 to 2019 10 22
23:59:59 user userA order-by time desc start-item 1 end-item 20
time, username, peerinfo, hostname, log-type: content
2019-10-22 10:00:03, ---, console, Hostname, SEC_LOG: SECURITY_LOG enabled
security log audit configuration 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 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG:
SECURITY_LOG deleted all security log successfully
……
```

The following example displays all security logs.

```
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
……
```

The following example exports security logs of the user “user A” from 00:00 on October 10, 2019 to 24:00 on October 22, 2019.

```
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
……
```

The following example runs the **copy** command to download log files.

```
Hostname#copy
```

```
tmp:mng/security_log/export_file/log_20191022_110410_535250.csv
tftp://192.168.1.1/security_log.csv
```

The following example displays the count of security logs of the user “user A” from 00:00 on October 10, 2019 to 24:00 on 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
```

Prompt Messages N/A

Platform Description N/A

9.8 show security-log config

Use this command to display security log configurations.

show security-log config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to display security log configurations, including whether log auditing is enabled, log capacity limit, log storage time, and everyday handling time for aged security logs.

Configuration Examples The following example displays security log configurations.

```
Hostname# show security-log config
Security-log audit: enable
```

```
Limit number: 10000
Store days: 180
Auto vacuum time: 03:00:00
```

Prompt Messages N/A

Platform Description N/A

9.9 show security-log statistics

Use this command to display security log statistics.

show security-log statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to display security log statistics, including the number of recorded logs and last deleted log. Detailed description is as follows:

The count of current recorded logs stored locally: xxx

The count of historical recorded logs stored locally: have written xxx, overwritten xxx

The count of aging logs stored locally: xxx

The record of last deletion: xxx

Configuration Examples The following example displays security log statistics.

```
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
```

Prompt Messages N/A

Platform Description N/A

9.10 show security-log info

Use this command to display statistics during log processing.

show security-log info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privilege EXEC mode

Default Level 15

Usage Guide Run this command to display statistics during log processing, including the number of logs received from service components, current cached logs, logs stored in flash memory and historical cached logs synchronized to flash memory, and next time to synchronize cached logs to flash memory. Detailed description is as follows:

The count of logs received successfully: xxx, the count of logs received unsuccessfully: xxx

The count of current cached logs: xxx

The count of logs stored in flash memory: xxx

The count of historical synchronization to falsh memory: xxx, the count of synchronization failures: xxx

The reason for last synchronization failure: xxx (The message is displayed only when a

synchronization failure occurred.)

Next time of synchronization to flash memory: HH:MM:SS

Configuration Examples The following example displays statistics during log processing.

```
Hostname# show security-log info
Receive log count: 2000, err 1
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
```

Prompt Messages N/A

Platform Description N/A

10 CWMP Commands

10.1 acs password

Use this command to configure the ACS password to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to cancel the configuration.

acs password { *password* | *encryption-type encrypted-password* }

no acs password

Parameter Description

Parameter	Description
password	Configures the ACS user password to be authenticated for the CPE to connect to the ACS.
encryption-type	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
encrypted-password	Specifies the password in encrypted form.

Defaults encryption-type: 0

encrypted-password: N/A

Command CWMP configuration mode

Mode

Usage Guide Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

- The command contains English letters in upper or lower case and numeric characters.
- Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs password 123
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

10.2 acs url

Use this command to configure the URL of the ACS to which the CPE will connect.

Use the **no** form of this command to restore the default setting.

acs url { *url* | **macc** }

no acs url

Parameter Description

Parameter	Description
url	Specifies the URL of the ACS.
macc	Connects to MACC.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements:

- The URL of the ACS is formatted as http://host[:port]/path or https://host[:port]/path.
- The URL of the ACS consists of at most 256 characters.

Use this command to connect to MACC quickly, achieving the same effect of running the following two commands:

- acs url https://cloud.ruijie.com.cn/service/acs
- cpe inform interval 30

Configuration Examples The following example specifies the URL of the ACS to http://10.10.10.1:8080/acs.

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs url http://10.10.10.1:8080/acs
Hostname(config-cwmp)#
```

The following example specifies the URL of the ACS to http://www.test.com/service/tr069servlet.

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs url http://www.test.com/service/tr069servlet
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.3 acs username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to restore the default setting.

acs username *username*

no acs username

Parameter

Parameter	Description

Description

username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Configuration Examples The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs username admin
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.

Use the **no** form of this command to disable this function.

cpe back-up [**delay-time** *seconds*]

no cpe back-up

Parameter Description

Parameter	Description
seconds	Specifies the delay for backup and restoration of the main program and configuration file of the CPE, in the range from 30 to 10,000 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode CWMP configuration mode

Usage Guide You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its main program or configuration file. Then when the CPE fails to connect to the ACS and breaks away from the NMS after its main program or configuration file is upgraded, the previous main program or configuration file of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong main program or configuration file.

Configuration Examples The following example disables the backup and restoration of the main program and configuration file of the CPE.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#no cpe back-up
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.4 cpe back-up

Use this command to enable the CPE backup function.
Use the **no** form of this command to restore the default setting.
cpe back-up [**delay-time** *seconds*]
no cpe back-up

Parameter Description

Parameter	Description
seconds	Sets the backup delay time (30-10,000 seconds).

Defaults The default is 60 seconds.

Command Mode CWMP configuration mode

Usage Guide After updrading main programs or configurations, CPE cannot communicate with ACS for wrong configuration delivery. Use this command to recover the previous programs and configurations.

Configuration Examples The following example disables the CPE backup function.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#no cpe back-up
Hostname(config-cwmp)#
```

Platform Description N/A

10.5 cpe inform

Use this command to configure the periodic notification function of the CPE.
Use the **no** form of this command to restore the default setting
cpe inform [**interval** *seconds*] [**start-time** *time*]
no cpe inform

Parameter Description

Parameter	Description
seconds	Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds.
time	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.

Defaults The default is 600 seconds.

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the periodic notification function of the CPE.

- If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval.
- If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions

between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.

Configuration Examples The following example specifies the periodical notification interval of the CPE to 60 seconds.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe inform interval 60
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.6 cpe password

Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the **no** form of this command to cancel the configuration.

cpe password { *password* | *encryption-type encrypted-password* }

no cpe password

Parameter Description

Parameter	Description
password	Configures the CPE user password to be authenticated for the ACS to connect to the CPE.
encryption-type	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
encrypted-password	Specifies the password in encrypted form.

Defaults encryption-type: 0

encrypted-password: N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs

to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

- The command contains English letters in upper or lower case and numeric characters.
- Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples

The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe password 123
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Platform Description

N/A

10.7 cpe source interface

Use this command to obtain an IP address on a specified interface and configure the URL of the CPE to which the ACS will connect. Use the **no** form of this command to restore the default configuration.

cpe source interface *interface-type interface-number* [**port** *port-number*]

no cpe source interface

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and number used to configure the URL of the CPE to which the ACS will connect.
port *port-number*	Port ID. The value range is from 1 to 65535. The default value is 7547.

Defaults

By default, an IP address is not obtained on a specified interface to configure the URL of the CPE to which the ACS will connect.

Command Mode CWMP configuration mode

Default Level 14

Usage Guide This command is incompatible with the **cpe url** command. You cannot configure the two commands at the same time. That is, if one command is configured, the other command must not be configured or deleted at first. When both commands are not configured, the CPE will automatically select a URL for the CPE according to the URL of the ACS.
The full name of the interface must be the interface name of the device, which is automatically populated when the CLI command is entered.
The default port number is 7547.

Configuration Examples The following example configures a URL of the CPE to which the ACS will connect on a Layer3 Ethernet interface.

```
Hostname#configure terminal
Hostname(config)#cwmp
Hostname(config-cwmp)# cpe source interface gigabitethernet 0/1 port 7547
```

Verification Run the **show cwmp configuration** command on the CPE device to check whether the configuration succeeds.

Prompt Messages If a wrong interface name is entered, the following message will be displayed.

```
% Invalid input detected at '^' marker.
```

If you have run the **cpe url** command to configure an IP address, the following message will be displayed.

```
Cpe url have been set by command cpe url, please clear it.
```

Common Errors N/A

Platform Description N/A

10.8 cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.
Use the **no** form of this command to restore default setting.
cpe url *url*
no cpe url

Parameter Description

Parameter	Description
url	Specifies the URL of the CPE.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements:

- The URL of the CPE is formatted as http://ip [: port]/ path.
- The URL of the CPE consists of at most 256 characters.

Configuration Examples The following example specifies the URL of the CPE to http://10.10.10.1:7547/acs.

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.9 cpe username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS.

Use the **no** form of this command to restore the default setting.

cpe username *username*

no cpe username

Parameter Description

Parameter	Description
username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Defaults N/A

Command CWMP configuration mode

Mode

Usage Guide Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Configuration Examples The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe username admin
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
cpe password	Configures the CPE password to be authenticated for the ACS to connect to the CPE.

Platform Description N/A

10.10 cwmp

Use this command to enable the CWMP function.

Use the **no** form of this command to disable this function.

cwmp

no cwmp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable the CWMP function.

Configuration Examples The following example disables the CWMP function.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Hostname(config)#no cwmp
Hostname(config)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.11 disable download

Use this command to disable the function of downloading main program and configuration files from the ACS. Use the **no** form of this command to restore the default setting.

disable download

no disable download

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can download main program and configuration files from the ACS.

Command Mode CWMP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the function of downloading main program and configuration files from the ACS.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#disable download
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.12 disable stun

Use this command to disable the auto negotiation function and the function to detect aging time of NAT session entries on a Simple Traversal of UDP over NATs (STUN) port. Use the **no** form of this command to enable the two functions.

disable stun { **port-adaptive** | **probe-agingtime** }

no disable stun { **port-adaptive** | **probe-agingtime** }

Parameter Description

Parameter	Description
port-adaptive	Indicates that the STUN port is enabled with auto negotiation.
probe-agingtime	Indicates that the STUN port is enabled with the function to detect aging time of NAT session entries.

Defaults By default, the auto negotiation function and the function to detect aging time of NAT session entries on an STUN port are disabled.

Command Mode CWMP configuration mode

Default Level 1

Usage Guide N/A

Configuration Examples The following example enables auto negotiation on an STUN port. The device automatically adapts to the STUN server on port 3478.

```
Hostname#configure terminal
Hostname(config)#cwmp
Hostname(config-cwmp)#no disable stun port-adaptive
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.13 disable upload

Use this command to disable the function of uploading configuration and log files to the ACS.

Use the **no** form of this command to restore the default setting.

disable upload

no disable upload

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can upload its configuration and log files to the ACS.

Command Mode CWMP configuration mode

Usage Guide Disables the function of uploading configuration and log files to the ACS.

Configuration Examples The following example disables the function of uploading configuration and log file to the ACS.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#disable upload
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.14 show cwmp configuration

Use this command to display the current configuration of CWMP.

show cwmp configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide

Configuration Examples The following example displays the current configuration of CWMP.

```
Hostname(config-cwmp)#show cwmp configuration
CWMP Status                  : enable
ACS URL                     : http://www.ruijie.com.cn/acs
ACS username                 : admin
ACS password                 : ******
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
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	The configuration status of CWMP.
ACS URL	URL of the ACS,
ACS username	ACS username to be authenticated for the CPE to connect to the ACS.
ACS password	ACS password to be authenticated for the CPE to connect to the ACS.
CPE URL	URL of the CPE.
CPE username	CPE username to be authenticated for the ACS to connect to the CPE.
CPE pass ord	CPE password to be authenticated for the ACS to connect to the CPE.
CPE inform status	Status of CPE periodical notification function.
CPE inform interval	CPE periodical notification interval.
CPE wait timeout	Timeout period of CPE sessions.
CPE inform start time	The start time of periodical notification.
CPE download status	Indicates whether to download main program and configuration files from the ACS.
CPE upload status	Indicates whether to upload configuration files and log files to the ACS.

CPE back up status	Indicates whether backup and restoration of the main program and configuration file is enabled.
CPE back up delay time	Delay time of the backup and restoration of the main program and configuration files.

Related Commands

Command	Description
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10.15 show cwmp status

Use this command to display the running status of CWMP

show cwmp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the running status of CWMP.

```
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
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	The configuration status of CWMP
Session status	The current status of the session between the CPE and the ACS
Last success session	The last success session type

Last success session time	The last success session time
Last fail session	The last failed session type
Last fail session time	The last failed session time
Session retry times	The number of session retransmission attempts

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.

Platform Description N/A

10.16 timer cpe-timeout

Use this command to configure the session timeout period of the CPE.

timer cpe- timeout *seconds*

no timer cpe-timeout

Parameter Description

Parameter	Description
seconds	Sets the session timeout, in the range from 10 to 600 in the unit of seconds.

Defaults By default, the session timeout period is 30 seconds.

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the session timeout period of the CPE.

The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

Configuration Examples The following example configures the session timeout period of the CPE to 50 seconds.

```
Hostname#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#timer cpe-timeout 50
Hostname(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

11 CA-MONITOR Commands

11.1 show power

Use this command to display power information including that of its basic condition, redundancy, allocation and version and etc.
show power**]**

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide This command is used to display power information

Configuration Examples N/A

Prompt Messages N/A

Platforms N/A

11.2 show fan

Use this command to display the operating status and speed adjustment mode of all the fan trays.
show fan [speed **]**

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide Use the show fan command without parameters to display the operating status and speed adjustment

mode of all the fan trays.

Configuration Examples The following example displays basic fan information.

```
Hostname#show fan
Fan-id Fan-type  Status
------ --------- ----------
1     RG_FAN    ok
2     RG_FAN    ok
Hostname#show fan speed
Fan-id Fan-type  Status    Speed(R/m) Speed-level
------ --------- ---------- ---------- -----------
1     RG_FAN    ok        N/A       1
2     RG_FAN    ok        N/A       1
Hostname#
```

Prompt Messages N/A

Platforms The display format may vary with devices.

11.3 show temperature

Use this command to display board temperature, threshold configuration and other information.
show temperature

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide N/A

Configuration Examples The following example displays the temperature and threshold configuration of all boards of the S2915-24GT4MS.

```
Hostname#show temperature
Slot    Card_type                    Temp_name             Current(C) Status
Warning(C) Critical(C)
```

```
------- -------- ------- ----------------------- ---------- ------ ----------
----------
0       S2915-24GT4MS-P            -L   board                18        ok
63        73
        S2915-24GT4MS-P-L   switch               34        ok      100     110
```

Prompt Messages Two new thresholds are added to the temperature display: **Warning** indicates the threshold of a minor alram, and **Critical** indicates the threshold of alarm verfication.

Platforms The display format may vary with devices.

12 ZAM Commands

12.1 show zam

Use this command to display the current configuration and status of ZAM.

show zam

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the current configuration and status of ZAM.

```
Hostname#
Hostname#show zam
ZAM state          : disable
ZAM status         : Now is idle
ZAM manage interface: Mgmt 0

Hostname#
```

Platform Description N/A

12.2 zam

Use this command to enable ZAM. Use the **no** form of this command to disable ZAM.

zam

Parameter Description

Parameter	Description
N/A	N/A

Defaults ZAM is disabled by default.

Command Mode	Global configuration mode
Usage Guide	

Configuration Examples	The following example enables ZAM.
	`Hostname(config)# zam`
	`Hostname(config)#`

Platform Description	N/A

13 Module Hot-plugging/ unplugging Commands

13.1 show manuinfo

Use this command to display asset information about all independent components in the system for asset management, including the chassis, fan, power, management board, and line card. The information covers the ID, slot number, name, serial number (SN), software and hardware version, and MAC address. Not all devices support display of the same information and only supported information is printed.

show manuinfo

Parameter Description

Parameter	Description
N/A	N/A

Defaults: N/A

Command Mode: Privileged EXEC mode

Usage Guide: This command is used to display asset information about all independent components in the system

Configuration Examples: The following example displays asset information of the single physical device.

```
Hostname#show manuinfo
Device 1
   Location:                Chassis
   Device name:             S2915-24GT4MS-P-L
   Device Serial Number:      1234942533311
   Hardware Version:         1.00
   Mac Address:             00.00.f8.23.01.10

Device 2
   Location:                Slot-0
   Device name:             S2915-24GT4MS-P-L
   Device Serial Number:      1234942533311
   Hardware Version:         1.00
   Software Version:         S2915-L_RGOS 11.4(1)B82, Release(09230219)
   Mac Address:             00.00.f8.23.01.10

Device 3
   Location:                Power 1
   Device name:             RG-POWER
```

```
   Device Serial Number:       N/A
   Hardware Version:          N/A

Device 4
   Location:                FAN 1
   Device name:              RG_FAN
   Device Serial Number:       N/A
   Hardware Version:          N/A
```

Platform Description N/A

13.2 show sysmac

Use this command to display the MAC address of the current system.

show sysmac

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the MAC address of the current system.

```
Hostname#show sysmac
00d0.f822.33e2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.3 show version module detail

Use this command to display the details of the module.

show version module detail [*slot-num*]

show version module detail [*device-id / slot-num]*

Parameter Description

Parameter	Description
slot-num	(Optional) Slot number.
device-id	(Optional) Device ID.

Defaults N/A

Command Mode Privileged EXEC mode.

Default Level 14

Usage Guide Use this command to display details of the module

Configuration Examples The following example displays details of the modules in the slot 2.

```
Hostname# show version module detail 2
Device  : 1
Slot : 0
   Soft Status : master
Online Module
Type    : S2915-24GT4MS-P-L
Ports   : 28
   Hardware version : 1.00
   Software version : S2915-L_RGOS 11.4(1)B82, Release(09230219)
   BOOT version    : 2019.10
Serial number   : 1234942533311
```

Platform Description N/A

13.4 show version slots

Use this command to display the online status of the modules.

show version slots [*slot-num*]

show version slots [*device-id / slot-num*]

Parameter Description

Parameter	Description
device-id	(Optional) Device ID.
slot-num	(Optional) Slot number.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Run this command to display the online status of the modules.

Configuration Examples The following example displays the online status of the modules.

```
Hostname# show version slots
Dev  Slot  Port Configured Module   Online Module    Software Status
  --- ---- ---- ---------------------------- ----------------------------
---------------
  1   0    28   S2915-24GT4MS-P-L          S2915-24GT4MS-P-L          master
```

Platform Description N/A

14 Supervisor Module Redundancy Commands

14.1 auto-sync time-period

Use this command to configure the auto-sync time-period of runing-config and startup-config when the dual supervisor module is redundant. Use the **no** form of this command to disable automatic synchronization for the dual supervisor modules. Use the **default** form of this command to restore the default automatic synchronization time period for the dual supervisor modules.

auto-sync time-period *value*

no auto-sync time-period

default auto-sync time-period

Parameter Description

Parameter	Description
value	Automatic synchronization time interval measured in seconds, in the range from one second to one month (2,678,400 seconds).

Defaults The default is one hour (3600 seconds) by default.

Command Mode Redundancy configuration mode

Usage Guide N/A

Configuration Examples The following example sets the automatic synchronization interval to 60 seconds.

```
Hostname(config)# redundancy
Hostname(config-red)# auto-sync time-period 60
```

```
Redundancy auto-sync time-period: enabled (60 seconds).
Hostname(config-red)# exit
```

The following example disables automatic synchronization.

```
Hostname(config)# redundancy
Hostname(config-red)# no auto-sync time-period
Redundancy auto-sync time-period: disabled.
Hostname(config-red)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.2 redundancy

Use this command to enter redundancy configuration mode.

redundancy

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enters redundancy configuration mode.

```
Hostname# config terminal
Hostname(config)# redundancy
Hostname(config-red)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.3 show redundancy states

Use this command to display the current redundancy state.

show redundancy states

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode / Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the redundancy states of active supervisor module.

```
Hostname> enable
Hostname# show redundancy states
Redundancy role: master
Redundancy state: realtime
Auto-sync time-period: 3600 s
```

The following example displays the redundancy state of the standby supervisor module.

```
Hostname> enable
Hostname# show redundancy states
Redundancy role: slave
Redundancy state: realtime
```

The following example displays the redundancy state of the candidate supervisor module.

```
Hostname> enable
Hostname# show redundancy states
Redundancy role: candidate
Redundancy state: none
```

Field	Description
role	The role of the supervisor module.
state	The state of the supervisor module.
Auto-sync time-period	Displayed on the active supervisor module. The configuration file synchronizes the time interval automatically. “disabled” indicates no automatic synchronization.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

15 PoE Management Commands

15.1 poe alloc-power

Use this command to set the allocation power for the port. Use the **no** or **default** form of this command to restore the default allocation power.

poe alloc-power *int*

no poe alloc-power

default poe alloc-power

Parameter Description

Parameter	Description
int	The maximum power, in the range from 0 to 30W.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the allocation power for port GigabitEthernet 0/1 to 20W.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe alloc-power 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.2 poe enable

Use this command to enable the power over Ethernet (PoE) function on the interface. Use the **no** form of this command to disable this function.

poe enable

no poe enable

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default,

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example disables the PoE function on port GigabitEthernet 0/1,

```
Hostname(config)# interface GigabitEthernet  0/1
Hostname(config-if-GigabitEthernet 0/1)# no poe enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.3 poe legacy

Use this command to enable non-standard PD compatibility. Use the **no** or **default** form of this command to restore the default setting.

poe legacy

no poe legacy

default poe legacy

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example enables non-standard compatibility for port GigabitEthernet 0/1.

```
Hostname(config)# interface GigabitEthernet  0/1
Hostname(config-if-GigabitEthernet 0/1)#  poe legacy
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.4 poe max-power

Use this command to set the maximum power for the port. Use the **no** or **default** form of this command to restore the default setting,

poe max-power *int*

no poe max-power

default poe max-power

Parameter Description

Parameter	Description
int	The maximum power, in the range from 0 to 30W. Note that this parameter is in the range from 0 to 15.4W on the system supporting 802.3af only. HPoE port ID is in the range from 0 to 90.

Defaults The maximum power is not set by default.

Command Mode Interface configuration mode

Usage Guide N/A.

Configuration Examples The following example sets the maximum power for port GigabitEthernet 0/1 to 20W.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#  poe max-power 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.5 poe mode

Use this command to set the PoE management mode. Use the **no** or **default** form of this command to

restore the default setting.

poe mode { **auto** | **energy-saving** | **static** }

no poe mode

default poe mode

Parameter Description

Parameter	Description
auto	Sets the power management mode to auto mode, the default mode.
energy-saving	Sets the power management mode to energy-saving mode, the optional mode,
static	Sets the power management mode to static mode,

Defaults The default mode is auto.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PoE management mode to energy-saving mode.

```
Hostname# configure
Hostname(config)# poe mode auto
Hostname(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.6 poe notification-control enable

Use this command to enable Trap notification in PoE MIB(RFC3621). Use the **no** or **default** form of this command to restore the default setting.

poe notification-control enable

no poe notification-control enable

default poe notification-control enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables Trap notification in PoE MIB(RFC3621).

```
Hostname(config)# poe notification-control enable
Hostname(config)# end
Hostname#write
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.7 poe pd-description

Use this command to set the PD descriptor for the port. Use the **no** or **default** form of this command to restore the default setting.

poe pd-description *pd-name*

no poe pd-description

default poe pd-description

Parameter Description

Parameter	Description
pd-name	PD descriptor name, a string no more than 32 characters.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PD descriptor for port GigabitEthernet 0/1.

```
Hostname# configure
Hostname(config)# interface GigabitEthernet  0/1
Hostname(config-if-GigabitEthernet 0/1)# poe pd-description ap220
Hostname(config-if-GigabitEthernet 0/1)# end
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

15.8 poe power-off time-range name

Use this command to configure scheduled power-on for the port. Use the **no** or **default** form of this command to restore the default setting.

poe power-off time-range *name*

no poe power-off time-range

default poe power-off time-range

Parameter Description

Parameter	Description
name	Time-range name.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the port GigabitEthernet 0/1 to be disabled from 8:30 to 17:30 on workday.

```
Hostname# configure
Hostname(config)# time-range poe-time
Hostname(config-time-range)# periodic weekdays 8:30 to 17:30
Hostname(config-time-range)# exit
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe power-off time-range poe-time
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.9 poe priority

Use this command to set the PoE priority for the port. Use the **no** or **default** form of this command to restore the default setting.

poe priority { **low** | **high** | **critical** }

no poe priority

default poe priority

Parameter Description

Parameter	Description
{ **low** | **high** | **critical** }	Priority level.

Defaults The default is low.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PoE priority for port GigabitEthernet 0/1 to critical.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe priority critical
Hostname(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.10 poe reserve-power

Use this command to set the reserve power for the system in energy-saving mode. Use the **no** or **default** form of this command to restore the default setting,

poe reserve-power *int*

no poe reserve-power

default poe reserve-power

Parameter Description

Parameter	Description
int	Reserve power percentage, in the range from 0 to 50.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the reserve power for the system to 10%.

```
Hostname(config)# poe reserve-power 10
Hostname(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.11 poe uninterruptible-power

Use this command to configure uninterruptible warm start, Use the **no** or **default** form of this command to restore the default setting.

poe uninterruptible-power

no poe uninterruptible-power

default no poe uninterruptible-power

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function takes effect when the device is started after the configuration is saved.

Configuration Examples The following example enables uninterruptible PoE for warm start and saves configuration.

```
Hostname(config)# poe uninterruptible-power
Hostname(config)# end
Hostname#write
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

15.12 poe warning-power

Use this command to set the power alarm threshold for the system. Use the **no** or **default f**orm of this command to restore the default setting,

poe warning-power *int*

no poe warning-power

default poe warning-power

Parameter Description

Parameter	Description
int	Power alarm threshold (percentage), in the range from 0 to 99.

Defaults The default is 99.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the power alarm threshold for the system to 80%.

```
Hostname(config)# poe waring-power 80
Hostname(config)# end
Hostname#write
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.13 show poe interface

Use this command to display PoE configuration and status of the specified port.

show poe interface *interface-name*

Parameter Description

Parameter	Description

interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the PoE configuration and status in interface GigabitEthernet 0/1.

```
Hostname#show poe interface GigabitEthernet 0/1
Interface             : Gi0/1
Power enabled          : enable
Power status           : on
Max power             : N/A
Allocate power         : N/A
Current power          : 14.8 W
Average power          : 14.8 W
Peak power            : 14.8 W
Voltage               : 53.5 V
Current               : 278 mA
PD class              : 4
Trouble cause          : None
Priority              : critical
Legacy                : off
Power-off time-range    : N/A
Power management       : auto
4pair status           : normal
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.14 show poe interfaces

Use this command to display PoE status or configuration of all ports.

show poe interfaces status

show poe interfaces configuration

Parameter

Parameter	Description

Description

status	Displays PoE status of all ports.
configuration	Displays PoE configuration of all ports.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display PoE status or configuration of all ports.

Configuration Examples The following example displays PoE status of all ports.

```
Hostname#show poe interfaces status
Interface Power   Power  Curr  Avg   Peak  Curr    Trouble PD    Port
         Control Status Power Power Power Current Cause   Class Voltage
-------------------------------------------------------------------------
Gi0/1    enable  on    14.8W 14.8W 14.8W 278mA   0      4     53.5V
Gi0/2    enable  on    28.4W 28.4W 28.4W 531mA   0      4     53.5V
Gi0/3    enable  on    14.9W 14.9W 14.9W 279mA   0      4     53.5V
Gi0/4    enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/5    enable  on    14.8W 14.8W 14.8W 278mA   0      4     53.5V
Gi0/6    enable  on    15.0W 15.0W 15.0W 281mA   0      4     53.5V
Gi0/7    enable  on    6.1W  6.1W  6.1W  115mA   0      4     53.5V
Gi0/8    enable  on    14.8W 14.8W 14.8W 277mA   0      4     53.5V
Gi0/9    enable  on    14.7W 14.7W 14.7W 276mA   0      4     53.5V
Gi0/10   enable  on    14.8W 14.8W 14.8W 278mA   0      4     53.5V
Gi0/11   enable  on    14.7W 14.7W 14.7W 275mA   0      4     53.5V
Gi0/12   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/13   enable  on    14.8W 14.8W 14.8W 278mA   0      4     53.5V
Gi0/14   enable  on    0.3W  0.3W  0.3W  7mA     0      4     53.5V
Gi0/15   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/16   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/17   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/18   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/19   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/20   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/21   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/22   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/23   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A   0.0V
Gi0/24   enable  off   0.0W  0.0W  0.0W  0mA     6      N/A
0.0V
```

The following example displays PoE configuration of all ports.

```
Hostname#show poe interfaces configuration
Interface  Power   Power   Max   Alloc  Port     Port   Power-off
```

```
          Control  Status  Power  Power  Priority  Legacy  Time-range
-------------------------------------------------------------------------
Gi0/1     enable   on      N/A    N/A    critical  off     N/A
Gi0/2     enable   on      N/A    N/A    critical  off     N/A
Gi0/3     enable   on      N/A    N/A    critical  off     N/A
Gi0/4     enable   off     N/A    N/A    critical  off     N/A
Gi0/5     enable   on      N/A    N/A    critical  off     N/A
Gi0/6     enable   on      N/A    N/A    high      off     N/A
Gi0/7     enable   on      N/A    N/A    high      off     N/A
Gi0/8     enable   on      N/A    N/A    high      off     N/A
Gi0/9     enable   on      N/A    N/A    high      off     N/A
Gi0/10    enable   on      N/A    N/A    high      off     N/A
Gi0/11    enable   on      N/A    N/A    high      off     N/A
Gi0/12    enable   off     N/A    N/A    high      off     N/A
Gi0/13    enable   on      N/A    N/A    low       off     N/A
Gi0/14    enable   on      N/A    N/A    low       off     N/A
Gi0/15    enable   off     N/A    N/A    low       off     N/A
Gi0/16    enable   off     N/A    N/A    low       off     N/A
Gi0/17    enable   off     N/A    N/A    low       off     N/A
Gi0/18    enable   off     N/A    N/A    low       off     N/A
Gi0/19    enable   off     N/A    N/A    low       off     N/A
Gi0/20    enable   off     N/A    N/A    low       off     N/A
Gi0/21    enable   off     N/A    N/A    low       off     N/A
Gi0/22    enable   off     N/A    N/A    low       off     N/A
Gi0/23    enable   off     N/A    N/A    low       off     N/A
Gi0/24    enable   off     N/A    N/A    low       off     N/A
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.15 show poe powersupply

Use this command to display the PoE power supply status.

show poe powersupply

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the PoE power supply status.

```
Hostname#show poe powersupply
Device member                : 1
Power management             : auto
PSE total power              : 1000W
PSE total power consumption    : 300W
PSE total remain power         : 700W
PSE peak power               : 0 W
PSE average power            : 0 W  PSE total powered port        : 0
PSE disconnect mode          : dc
PSE reserve power            : 0%
PSE available reserve power    : 0 W
PSE warning power            : 90%
PSE class lldp               : disable
PSE uninterruptible-power      : disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

16 PKG_MGMT Commands

16.1 clear storage

Use this command to remove an installation package on the local device.

clearstorage[*url*]

Parameter Description

Parameter	Description
url	A local *url* directory or full path name indicates where the installation package is stored

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to remove an installation package or all packages in a directory and all installation packages on the local device.

Configuration Examples

```
Hostname#clear storage
Remove the whole storage directory?[y/n]y
Hostname#clear storage usb0
Remove the file or directory usb0 from the storage?[y/n]y
Hostname#
```

Verification Check specified *url*

Platforms N/A

16.2 show component

Use this command todisplay all components already installed on current device and their information.

show component [*component _name*]

Parameter Description

Parameter	Description
component _name	Name of the components When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components.

	When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component isintact, and check whether this component works properly.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command includes one with *component_name* and one without *component_name*. During upgrade, it requires users to understand all components installed on current device and their version information before components deletion. This needs to use the **show component** command without *component_name*. The **show component** command with *component_name* is used to obtain details of the corresponding component. The detailed information enables users to easily realize components' operation and damage. It is significant to insure their troubleshooting, security and reliability.

Some components in use will change their defaults files. Though this is more possibly normal than malicious, the **show component** command is used only to judge whether component files change in use. It is unable to distinguish natural damage from malicious one. It depends on users to make a further judgment.

Configuration Examples The following example displays all components already installed and their information.

```
Hostname# show component
Package :sysmonit
    Version:1.0.1.23cd34aa     Build time: Wed Dec  7 00:58:56 2013
    Size:12877  Install time :Wed   Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
------------------------------------------------------------------
Package:bridge
    Version:2.0.1.37cd5cda     Build time: Wed Dec  7 00:54:56 2013
    Size:23245  Install time :Wed   Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
------------------------------------------------------------------
```

This command is used to obtain all components already installed on the device and theirbasic information. The information offers a basis for users to decide whether to upgrade or delete components.

Field	Description
Package	Name of the component
Version	Version number of the component

Build time	Compilation time of the component on the server
Size	Content size of the component
Install time	Installation time of the component
Description	Simple functional description of the component
Required packages	Name of required packages

The following example displays the information of specified components already installed on the device.

```
Hostname# show componentbridge
package:bridge
    Version: 2.3.1.1252ea      Build time: Wed Dec  7 00:54:56 2013
    Size:26945  Install time : Wed  Mar 19:23:15 2012
    Description:this is a bridge package
    Required packages: None
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
    /sbin/bridge

   Package file validate: [OK]
   Required relationship verify: [OK]
```

The other information except the basic information of components is listed as follows.

Field	Description
Package file validate	Checks whether the component filesare intact. “OK” is displayed when all component files work properly; “ERR” is displayed together with their names when some component files are lost or revised.
Required package	Lists all required packages of the component. “OK” is labeled if required components are already installed; “ERR” is labeled if not together with detailed description about their names and versions.
Package files	Lists all files contained in the package.

Prompt Messages The execution is successful with all components information displayed.

```
Package :sysmonit
    Version:1.0.1.23cd34aa     Build time: Wed Dec  7 00:58:56 2013
    Size:12877  Install time :Wed   Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
```

```
------------------------------------------------------------------
Package:bridge
    Version:2.0.1.37cd5cda     Build time: Wed Dec  7 00:54:56 2013
    Size:23245  Install time :Wed   Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
------------------------------------------------------------------
```

16.3 show upgrade auto-sync

Use this command to display related auto-sync configuration on the device.

show upgrade auto-sync

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to display the auto-sync upgrade configuration in the system including the policy, range and upgrade package's path.

Prompt Messages The auto-sync information of the system is displayed after running.

```
Hostname#show upgrade auto-sync
   auto-sync policy: coordinate
   auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin
```

16.4 show upgrade file

Use this command to display the information of the installation package files in the device file system.

show upgrade file *url*

Parameter Description

Parameter	Description
url	The local *url* path indicates where an installation package file is stored.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to preview main messages of an installation package after it is downloaded into local file system.

Configuration Examples The following example displays the information of an installation package file.

```
Hostname# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name    : bridge
Version:1.0.1.23cd34aa
Package type     : common component
Support target   : eg1000m
Size            : 26945
Build time       : Wed Dec  7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

This command is used to obtain the information in the package.

Field	Description
Name	Name of the package
Version	Version of the package
Package type	Type of the package
Support target	Supported product description
Size	Content size of the package
Build time	Compilation time of the package
Install date	Installation time of the package
Description	Description of the package
Package files	All contents in the package

Prompt Messages The package information is displayed after running.

```
Name    : bridge
Version:1.0.1.23cd34aa
Package type     : common component
Support target   : eg1000m
Size            : 26945
Build time       : Wed Dec  7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
```

```
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
   /sbin/bridge
```

16.5 show upgrade history

Use this command to display the upgrade history.

show upgrade history

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Configuration Examples The following example displays the upgrade history.

```
Hostname#show upgrade history
Last Upgrade Information:
   Time:        2014-08-31 12:15:03
   Method:      LOCAL
Package Name:S29_RGOS 11.0(1)B1_install.bin
Package Type: Distribution
```

Prompt Messages N/A

Platforms N/A

16.6 upgrade

Use this command to install and upgrade an installation package in the local file system.

upgrade *url*[**force**]

Parameter Description

Parameter	Description
url	The local path indicates where an installation package is stored. This command is used to upgrade an installation package on the

	device.
force	Mandatory upgrade

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is applicable to installation packages of all subsystem components, chassis devices, and feature components. Before its use, run the **copy** command to copy feature packages into the file system in the device.
When there is no specified range of parameters, the command is used to upgrade the matched system components according to the auto-sync configuration.

Configuration Examples

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.
Run the **show component** command to check whether the upgrade of a feature component is successful. upgrading a feature component

Prompt Messages The prompt message of successful running is displayed.

```
Upgrade info [OK]
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

16.7 upgrade auto-sync package

Use this command to configure the path for the auto-sync upgrade.

upgrade auto-sync package *url*

Parameter Description

Parameter	Description
url	The path of installation package.

Defaults The default is the last upgrade path.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide It is recommended to use default settings.

Configuration Examples

Verification Run the **show upgrade auto-sync** command to display current auto-sync policy.
If *url* provides normal path, run the **stat** command to check whether it can be accessed.

Prompt Messages

16.8 Upgrade auto-sync policy

Use this command to set an auto-sync policy for the system.

upgrade auto-sync policy [**none** | **compatible** | **coordinate**]

Parameter Description

Parameter	Description
none	No auto-sync upgrade
compatible	Performs auto-synchronization based on the sequential order of versions.
coordinate	Synchronizes with the version based on the system upgrade patch stored on the supervisor module.

Defaults **coordinate**

Command Privileged EXEC mode

Mode

Default Level 2

Usage Guide Check whether the upgrade package is ready before using the command.

Configuration Examples The following example sets the auto-sync policy of the device based on the version of supervisor modules.

```
Hostname# upgrade auto-sync policy coordinate
```

Verification Display the current policy for auto-sync upgrade by running the **show upgrade auto-sync** command.

Prompt Messages The prompt message of successful running is displayed.

```
Upgrade auto-sync policy is set as coordinate.
```

16.9 upgrade auto-sync range

Use this command to set the range of auto-sync upgrade.

upgrade auto-sync range [**chassis**]

Parameter Description

Parameter	Description
chassis	Auto-sync version upgrade in the range of chassis

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide N/A

Configuration Examples The following example installs the auto-sync upgrade in the range of chassis.

```
Hostname# upgrade auto-sync range chassis
```

Verification Run the **show upgrade auto-sync** command to display the range of current auto-sync upgrade.

Prompt Messages

```
N/A
```

16.10 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

upgrade download tftp:/*path* [**force**]

Parameter Description

Parameter	Description
path	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
force	Enforces upgrade.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is applicable to installation packages of all subsystem components, chassis devices, and feature components. This command is used to perform automatic installation, copy and upgrade of files.

Configuration Examples The following example upgrades the main package.

```
Hostname# upgrade download
tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%
 Upgrade info [OK]
        Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
        Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
 Upgrade processing is 100%
Reload to take effect!
```

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful.

Prompt Messages

The prompt message of successful running is displayed.

```
Upgrade info [OK];
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

16.11 upgrade download ftp

Use this command to download, install and upgrade installation packages from the ftp server.

upgrade download ftp:/*path* [**force**]

Parameter Description

Parameter	Description
path	The path of installation packages on the ftp server This command is downloaded and upgraded automatically from the server.
force	Enforces upgrade.

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command is applicable to installation packages of all subsystem components, chassis devices, and feature components. This command is used to perform automatic installation, copy and upgrade of files.

Configuration Examples

The following example upgrades the main package.

```
Hostname# upgrade download
ftp://username:password@192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
 Upgrade processing is 10%
```

```
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
        Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
        Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload to take effect!
```

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.
Run the **show patch** command to check whether the hot patch is isntalled successfully.

Prompt Messages The prompt message of successful running is displayed.

```
Upgrade info [OK];
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

Prompt Messages N/A

Platforms N/A

17 SF-APP

17.1 auto-config-recovery

Use this command to enable the automatic configuration restore function. Use the **no** or **default** form of this command to restore the default setting.

auto-config-recovery

no/default auto-config-recovery

Parameter Description

Parameter	Description
N/A	N/A

Defaults The automatic configuration restore function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The automatic configuration restore function is disabled by default. This function is enabled only after running the **auto-config-recovery** command.

Configuration Examples The following example disables the automatic configuration restore function.

```
Hostname(config)# no auto-config-recovery
```

Verification Run the **show run** command to check whether the **auto-config-recovery** configuration exists.

Prompt Messages N/A

Common Errors N/A

Platform N/A

Description

17.2 auto-collect upload interval

Use this command to configure the interval to collect MIB node information automatically. Use the **no** or **default** form of this command to restore the default setting.

auto-collect upload interval *time*

no/default auto-collect upload interval

Parameter Description

Parameter	Description
time	The interval to automatically collect MIB node information in seconds. The value range is from 30 to 172800, that is, from 30 seconds to 2 days.

Defaults The default interval to automatically collect MIB node information is 1800 seconds (30 min).

Command Mode Global configuration mode

Default Level 14

Usage Guide By default, the system collects MIB node information every 1800 seconds and sends compressed files to SF-APP. You can set different time intervals as needed. Run the **no** or **default** form of this command to restore the default setting.

Configuration Examples The following example sets the interval to automatically collect MIB node information to 300 seconds.

```
Hostname(config)# auto-collect upload interval 300
```

Verification Run the **show run** command to check whether the **auto-collect upload interval** configuration exists.

Prompt Messages N/A

Common Errors N/A

Platform N/A

Description

17.3 auto-collect upload url

Use this command to specify a path to upload files to a server. Use the **no** or **default** form of this command to restore the default setting.

auto-collect upload url *url*

no/default auto-collect upload url

Parameter Description

Parameter	Description
url	The path to upload files to a server.

Defaults No path to upload files to a server is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Without a path to upload files to the server, the system does not collect MIB node information. You can delete server paths to save system resources when data collection is not required.

Configuration Examples The following example configures the server path.

```
Hostname(config)# auto-collect upload url http://172.30.33.97/vm_share/
```

Verification Run the **show run** command to check whether the **auto-collect upload url** configuration exists.

Prompt Messages N/A

Common Errors A server path must start with “http://” or “http://”. The administrator check specific path information to ensure the validity of a path. The system only checks whether the path starts with “http://” or “http://”.

Platform Description N/A

17.4 auto-collect upload table

Use this command to collect MIB node data in real time.

auto-collect upload table {**arp-table** | **interface-table** | **mac-table** | **system-information** | **all**}

Parameter Description

Parameter	Description
arp-table	Collects MIB node information of ARP tables.
interface-table	Collects MIB node information of interface tables.
mac-table	Collects MIB node information of MAC address tables.
system-information	Collects MIB node information except the preceding three types of information.
all	Collects all MIB node information.

Defaults No path to upload files to a server is configured by default.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Configure the corresponding command to trigger the system to collect relevant MIB node information. The command only collects the information of MIB nodes listed in a metropolitan area network (MAN) for general education. The unlisted MIB nodes are not in the collection range of this command. Specifies different parameters to trigger information collection. Ensure that the server path is specified on the device before running this command to collect information. Because this is not a configuration command, you cannot run the **show run** command to display its configuration.

Configuration Examples The following example enables the system to collect MIB node information of MAC address tables in real time.

```
Hostname# auto-collect upload table mac-table
```

Verification The system has collected corresponding MIB node information and sent packages to the specified server path.

Prompt N/A

Messages

Common Errors	N/A
Platform Description	N/A

Ethernet Configuration Commands

1. Interface Commands
2. MAC Address Commands
3. Aggregate Port Commands
4. VLAN Commands
5. Voice VLAN Commands
6. MSTP Commands
7. LLDP Commands
8. QinQ Commands
9. ERPS Commands

1 Interface Commands

1.1 bandwidth

Use this command to set the bandwidth on the interface. Use the **no** form of this command to restore the default setting.

bandwidth *kilobits*

no bandwidth

Parameter Description

Parameter	Description
kilobits	Bandwidth per second, in the unit of Kbps.

Defaults If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.

Command Mode Interface configuration mode

Usage Guide This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.

Configuration Examples The following example sets the bandwidth on the interface to 64 Kbps.

```
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# bandwidth 64
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 carrier-delay

Use this command to set the carrier delay on the interface. Use the no form of this command to restore the default value.

carrier-delay { [*milliseconds*] *num* | **up** [*milliseconds*] *num* **down** [*milliseconds*] *num*}

no carrier-delay

Parameter Description

Parameter	Description
num	(Optional) in the range from 0 to 60 in the unit of seconds.

milliseconds	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
up	(Optional) Configures the delay after which DCD changes from Down to Up in status.
down	(Optional) Configures the delay after which DCD changes from Up to Down in status.

Defaults The default is 2 seconds.

Command Mode Interface configuration mode

Usage Guide This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status or vice versa. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

Configuration Examples The following example sets the carrier delay of serial interface to 5 seconds.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config)# carrier-delay 5
```

The following example sets the carrier delay of serial interface to 100 milliseconds.

```
Hostname(config)# interface GigabitEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)#carrier-delay milliseconds 100
```

The following example sets the DCD delay from Down to Up in status to 100 milliseconds and from Up to Down to 200 milliseconds.

```
Hostname(config)# interface GigabitEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# carrier-delay up milliseconds 100
down milliseconds 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 clear counters

Use this command to clear the counters on the specified interface.

clear counters [*interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

Configuration Examples The following example clears the counters on interface gigabitethernet 1/1.

```
Hostname# clear counters gigabitethernet 1/1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.4 clear interface

Use this command to reset the interface.

clear interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Configuration The following example resets the interface gigabitethernet 1/1.

Examples

```
Hostname# clear interface gigabitethernet 1/1
```

Related Commands

Command	Description
shutdown	Disables the interface.

Platform Description N/A

1.5 description

Use this command to configure the alias of interface. Use the **no** form of this command to restore the default setting.

description *string*

no description

Parameter Description

Parameter	Description
string	Interface alias

Defaults No alias is configured by default.

Command Mode Interface configuration mode.

Usage Guide Use **show interfaces** to display the interface information, including the alias.

Configuration Examples The following example configures the alias of interface.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# description GBIC-1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

duplex { **auto** | **full** | **half** }

no duplex

Parameter Description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Defaults The default is **auto**,

Command Mode Interface configuration mode.

Usage Guide The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Configuration Examples The following example specifies the duplex mode for the interface.

```
Hostname(config-if)# duplex full
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.7 eee enable

Use this command to enable Energy Efficient Ethernet (EEE) on the interface.

eee enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to achieve EEE on the interface in Low Power Idle(LPI) mode,

Configuration The following example enables EEE on GigabitEthernet 0/1.

Examples

```
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# eee enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.8 errdisable recovery

Use this command to recover the interface in violation.

errdisable recovery [**interval** *time*]

Parameter Description

Parameter	Description
interval *time*	Time for the command to take effect. The range is from 30 to 86,400 seconds.

Defaults By default, it is disabled.

Command Mode Global configuration mode.

Usage Guide Use the command to recover the port that triggers violation after being configured with the **violation shutdown** command.

Configuration Examples The following example recovers the violation interface gigabitethernet 1/1.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# errdisable recovery
```

Related Commands

Command	Description
switchport port-security violation shutdown	Configures the port security violation to shut down.

Platform Description N/A.

1.9 fiber alarm-detect enable

Use this command to enable the optical module alarm detection function.

fiber alarm-detect enable

Use this command to disable the optical module alarm detection function.

no fiber alarm-detect enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, it is disabled.

Command Mode Global configuration mode.

Default Level 14

Usage Guide When the optical module alarm detection function is enabled, the device will periodically monitor the status of the optical module on the interface. When an event such as optical module plugging/exception/exception recovery occurs, a TRAP will be sent and vice versa.

Configuration Examples 1: The following example enables the optical module alarm detection function on the device.

```
Ruijie(config)# fiber alarm-detect enable
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.10 fiber alarm-detect period

Use this command to configure the alarm period for the occurrence and recovery of exception events in the optical module.

fiber alarm-detect period *minutes*

Use this command to restore the default configuration.

no fiber alarm-detect period

Parameter Description

Parameter	Description

minutes	Alarm period for the occurrence and recovery of exception events in the optical module, in minutes. Range: 1-1440

Defaults The default value is 10 minutes.

Command Mode Global configuration mode.

Default Level 14

Usage Guide Optical module exception and exception recovery events will be notified within a period of time. Exception events will be notified periodically, while exception recovery events will be notified only once.

Configuration Examples 1: The following examples sets the alarm detection period.
Ruijie(config)# fiber alarm-detect period 720

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.11 fiber alarm-detect repeat-mode

Use this command to enable the optical module alarm detection repeat notification function.
fiber alarm-detect repeat-mode { **on** | **off** }
Use this command to restore the default configuration.
no fiber alarm-detect repeat-mode

Parameter Description

Parameter	Description
on	Enables repeat notification mode.
off	Disables repeat notification mode.

Defaults By default, the repeat notification mode is enabled. That is, the optical module alarm is periodically notified.

Command Global configuration mode.

Mode

Default Level 14

Usage Guide Optical module exception and exception recovery events will be notified within a period of time. Exception events will be notified periodically. You can disable the periodic notification function by disabling the repeat notification mode switch.

Configuration Examples The following examples disables the alarm periodic notification function.

```
Ruijie(config)# fiber alarm-detect repeat-mode off
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.12 fiber antifake enable

Use this command to enable or disable the optical module antifake detection. Use the **no** form of this command to restore the default setting.

fiber antifake {ignore | enable}

no fiber antifake enable

Parameter Description

Parameter	Description
ignore	N/A
enable	

Defaults By default, optical module antifake detection is disabled.

Command Mode Global configuration mode

Usage Guide If the optical module antifake detection is enabled by default, when a non-original optical module is inserted, alarm logs are printed.

Configuration Examples The following example enables the optical module antifake detection.

```
Hostname(config)# fiber antifake enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.13 flowcontrol

Use this command to enable or disable the flow control. Use the **no** form of this command to restore the default setting.

flowcontrol { **auto** | **off** | **on**}

no flowcontrol

Parameter Description

Parameter	Description
auto	Self-negotiates the flow control.
off	Disables the flow control.
on	Enables the flow control.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide Use the **show interfaces** command to display the flow control configuration.

Configuration Examples The following example enables flow control on fastEthernet port 1/1.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# flowcontrol on
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.14 interface

Use this command to enter the interface configuration mode.

interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	The interface type.
interface-number	The interface ID.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is used to enter interface configuration mode. The user can modify the interface configuration in the interface configuration mode.

Configuration Examples The following example enters configuration mode on Aggregateport 1.

```
Hostname(config)# interface Aggregateport 1
Hostname(config-if-Aggregateport 1)#
```

The following example enters configuration mode on GigabitEthernet 1/2.

```
Hostname(config)# interface GigabitEthernet 1/2
Hostname(config-if-GigabitEthernet 1/2)#
```

The following example configuration mode on VLAN 1.

```
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.15 interface range

Use this command to enter interface configuration mode on multiple interfaces.

interface range { *port-range* | **macro** *macro_name* }

Use this command to define the macro name of the **interface range** command.

define interface-range *macro_name*

Parameter

Parameter	Description

Description

port-range	The interface type and ID range, entered in the form of *interface-type slot-number/interface-number*. The interface can be either an Ethernet physical interface or a loopback interface.
macro *macro_name*	The macro name which represents the interface range.

Defaults The **interface range** command is disabled by default.

Command Mode Global configuration mode

Usage Guide Use the define interface-range command to define a range of interfaces as the macro name, and then use the **interface** range macro macro_name command to enter interface configuration mode on multiple interfaces.

Configuration Examples The following example enters interface configuration mode on multiple interfaces by setting the interface range.

```
Hostname(config)# interface range gigabitEthernet 0/0, 0/2
Hostname(config-if-range)# bandwidth 100
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
Hostname(config)# define interface-range route1 gigabitEthernet 0/0-2
Hostname(config)# interface range macro route1
Hostname(config-if-range)# bandwidth 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.16 line-detect

Use this command to detect the cable connection status.

line-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Interface configuration mode.

Mode

Usage Guide This command is used to detect the line status and locate the problem in case of a line failure, for example, the line is torn down.

Configuration Examples The following example detects the cable connection status on gigabitEthernet 0/1.

```
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#line-detect

Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok        1
pair state     length(meters)
---- ---------- --------------
B    Ok        2
pair state     length(meters)
---- ---------- --------------
C    Short     1
pair state     length(meters)
---- ---------- --------------
D    Short     1
```

Field	Description
pairs	Number of line pairs included. For example, the twisted pair includes four pairs of lines.
state	Status of the current line pair: OK, Short or Open. In general, the 100M twisted pairs A and B are OK, C and D are Short. The 1000M twisted pairs A, B, C and D are all OK.
length	Length of the line in meter. Only the length of the line pair whose status is OK takes effect. Since the length is calculated based on the transmission time of signal, there may have a certain difference. The length of the line pair whose status is Short or Open is the length from the port to the faulty point.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.17 load-interval

Use this command to set the interval for calculating load on the interface. Use the **no** form of this command to restore the default setting.

load-interval *seconds*

no load-interval

Parameter Description

Parameter	Description
seconds	In the range from 5 to 600 in the unit of seconds.

Defaults The default is 10.

Command Mode Interface configuration mode

Usage Guide This command is used to set the interval for calculating load on the interface. In general, the numbers of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the **show interface gigabitEthernet 0/1** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

Configuration Examples The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# load-interval 180
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.18 logging

Use this command to print information on the interface.

logging [**link-updown** | **error-frame** | **link-dither**]

Parameter Description

Parameter	Description
link-updown	Prints the status change information.

error-frame	Prints the error frame information.
link-dither	Prints the oscillation information.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example prints information on the interface.

```
Hostname(config)# logging link-updown
Hostname(config)# logging error-frame
Hostname(config)# logging link-dither
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.19 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter Description

Parameter	Description
num	64-9216

Defaults The default is 1500.

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command is used to set the maximum transmission unit (MTU) supported on the interface, that is, the maximum data length of the link layer. Currently, the MTU can only be set on a physical port.

Configuration Examples 1: The following example sets the MTU supported on=GigabitEthernet 1/1 to 9000.

```
Ruijie(config)# interface GigabitEthernet 1/1
```

```
Ruijie(config-if-GigabitEthernet)# mtu 9000
```

Verification 1: Run the **show interfaces** command to view the MTU on the interface.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.20 negotiation mode

Use this command to enable or disable auto-negotiation mode. Use the no form of this command to restore default configuration.
negotiation mode { **on** | **off** }
no negotiation mode

Parameter Description

Parameter	Description
on	Enables auto-negotiation.
off	Disables auto-negotiation.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Default Level 14

Usage Guide In general, the auto-negotiation status is determined by interface speed, duplex, flow control and auto-negotiation factor mode.

Configuration Examples The following example enables auto-negotiation mode on interface GigabitEthernet 1/1.

```
Hostname(config)# interface GigabitEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# negotiation mode on
```

Verification 1: Run the **show interfaces** command to view the auto-negotiation status of the interface.

Prompt Messages N/A

Command Errors N/A

Platform Description N/A

1.21 physical-port dither protect

Use this command to enable oscillation protection on the port.

physical-port dither protect

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide After you configure the **physical-port dither protect** command, the port will be shut down when the oscillation occurs for certain times.

If oscillation occurs on the port for 6 times within 2 seconds, a syslog will be printed. If syslog is printed for 10 consecutive times, the port will be shut down. If oscillation occurs on the port for over 10 times within 10 seconds, a syslog will be printed but the port will not be shut down.

Configuration Examples The following example enables oscillation protection on the port.

```
Hostname(config)# physical-port dither protect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.22 protected-ports route-deny

Use this command to configure L3 routing between the protected ports. Use the **no** form of this command to restore the default setting.

protected-ports route-deny

no protected-ports route-deny

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The ports that are set as the protected ports can route on L3. Use this command to deny the L3 communication between protected ports. Use the **show running-config** command to display configuration.

Configuration Examples The following example configures L3 routing between the protected ports.

```
Hostname(config)# protected-ports route-deny
```

Related Commands

Command	Description
show running-config	Displays the protected ports route-deny configuration.

Platform Description N/A

1.23 show eee interfaces status

Use this command to display interface EEE status.

show eee interfaces { *interface-type interface-number* | *status* }

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and ID.
status	All interface EEE status.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the interface is specified, the EEE status of the specified interface is displayed; otherwise, the EEE status of all interfaces is displayed.

Configuration Examples

The following example displays EEE status of interface GigabitEthernet 0/1.

```
Hostname#show eee interface gigabitEthernet 0/1
Interface              : Gi0/1
EEE Support            : Yes
Admin Status           : Enable
Oper Status            : Disable
Remote Status          : Disable
Trouble Cause          : Remote Disable
```

Field	Description
EEE Support	Whether EEE is supported
Admin Status	Configuration status
Oper Status	Operation status
Trouble Cause	Trouble cause

The following example displays EEE status of all interfaces.

```
Hostname#show eee interface status
Interface EEE    Admin    Oper    Remote   Trouble
         Support Status   Status   Status   Cause
--------- ------- -------- -------- -------- --------------------
Gi0/1     Yes    Enable   Disable  Disable   Remote Disable
Gi0/2     Yes    Enable   Disable  Unknown   None
Gi0/3     Yes    Enable   Enable   Enable    None
Gi0/4     Yes    Enable   Enable   Enable    None
Gi0/5     Yes    Enable   Enable   Enable    None
Gi0/6     Yes    Enable   Enable   Enable    None
Gi0/7     Yes    Enable   Enable   Enable    None
Gi0/8     Yes    Enable   Enable   Enable    None
Gi0/9     Yes    Enable   Enable   Enable    None
Gi0/10    Yes    Enable   Enable   Enable    None
Gi0/11    Yes    Enable   Enable   Enable    None
Gi0/12    Yes    Enable   Enable   Enable    None
Gi0/13    Yes    Enable   Enable   Enable    None
Gi0/14    Yes    Enable   Enable   Enable    None
Gi0/15    Yes    Enable   Enable   Enable    None
Gi0/16    Yes    Enable   Enable   Enable    None
Gi0/17    Yes    Enable   Enable   Enable    None
Gi0/18    Yes    Enable   Enable   Enable    None
Gi0/19    Yes    Enable   Enable   Enable    None
Gi0/20    Yes    Enable   Enable   Enable    None
Gi0/21    Yes    Enable   Enable   Enable    None
Gi0/22    Yes    Enable   Enable   Enable    None
Gi0/23    Yes    Enable   Enable   Enable    None
Gi0/24    Yes    Enable   Enable   Enable    None
Gi0/25    No     -        -        -           -
```

```
Gi0/26    No      -       -       -           -
Gi0/27    No      -       -       -           -
Gi0/28    No      -       -       -           -
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.24 show interfaces

Use this command to display the interface information and optical module information.

show interfaces [*interface-type interface-number*] [**description | switchport | trunk**]

Parameter Description

Parameter	Description
interface-id interface-number	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
description	The description of the interface, including the link status.
switchport	Layer 2 interface information.
trunk	Trunk port, applicable for physical port and aggregate port.

Defaults

Command Mode Privileged EXEC mode.

Usage Guide This command is used to show all basic information if no parameter is specified.

Configuration Examples The following example displays the interface information when the Gi0/1 is a Trunk port.

```
SwitchA#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
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
```

```
   Output queue 0/0, 0 drops;
   Input queue 0/75, 0 drops
  Switchport attributes:
   interface's description:""
   medium-type is copper
   lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
   Priority is 0
   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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
 Port-type: trunk
  Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
  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 when the Gi0/1 is an Access port.

```
SwitchA#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
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
```

```
   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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: access
Vlan id : 2
  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 layer-2 interface information when the Gi0/1 is a Hybrid port.

```
SwitchA#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
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: hybrid
```

```
Tagged vlan id:2
Untagged vlan id:none
  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 layer-2 information of the Gi0/1.

```
Hostname# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
--------- ---------- --------- ------ ------ ---------
GigabitEthernet 0/1 enabled Access 11  Disabled  ALL
```

Related Commands

Command	Description
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Selects the interface and enter the interface configuration mode.
interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
shutdown	Disables the interface.
speed	Configures the speed on the port.
switchport priority	Configures the default 802.1q interface priority.
switchport protected	Configures the interface as a protected port.

Platform Description N/A

1.25 show interfaces counters

Use this command to display the received and transmitted packet statistics.

show interfaces [*interface-type interface-number*] **counters** [**increment** | **errors** | **rate** | **summary**] [*up* | *down*]

Parameter Description

Parameter	Description
interface-type	(Optional) The interface type and ID.

interface-number	
increment	Displays the packet statistics increased during the last sample interval.
errors	Displays error packet statistics.
rate	Displays packet receiving and transmitting rate.
summary	Displays packet statistics summary.
up	(Optional) Displays the port up statistics.
down	(Optional) Displays the port down statistics.

Defaults N/A

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, the packet statistics on all interfaces are displayed.

Configuration Examples The following example displays packet statistics on interface GigabitEthernet 0/1.

```
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
```

Rxload refers to the receive bandwidth usage and Txload refers to the Tx bandwidth usage. InPkts is the total number of receive unicast, multicast and broadcast packets. OutPkts is the total number of transmit unicast, multicast and broadcast packets.

Packet increment in last sampling interval (5 seconds) represents the packet statistics increased during the last sample interval (5 seconds).

The following example displays the packet statistics on interface GigabitEthernet 0/1 increased during the last sample interval.

```
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 error packet statistics on interface GigabitEthernet 0/1.

```
Hostname#show interfaces GigabitEthernet 0/1 counters increment
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
```

UnderSize is the number of valid packets smaller than 64 bytes.
OverSize is the number of valid packets smaller than 1518 bytes.
Collisions is the number of colliding transmit packets.
Fragments is the number of packets with CRC error or frame alignment error which are smaller than 64 bytes.
Jabbers is the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.
CRC-Align-Err is the number of receive packets with CRC error.
Align_Err is the number of receive packets with frame alignment error.
FCS-Err is the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on interface GigabitEthernet 0/1.

```
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
```

Sampling Time is the time when packets are sampled. Input rate is packet receiving rate and Output rate is packet transmitting rate.

The following example displays packet statistics summary on interface GigabitEthernet 0/1.

```
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
```

InOctets is the total number of packets received on the interface. InUcastPkts is the number of unicast packets received on the interface. InMulticastPkts is the number of multicast packets

received on the interface. InBroadcastPkts is the number of broadcast packets received on the interface.
OutOctets is the total number of packets transmitted on the interface. OutUcastPkts is the number of unicast packets transmitted on the interface. OutMulticastPkts is the number of multicast packets transmitted on the interface. OutBroadcastPkts is the number of broadcast packets transmitted on the interface.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.26 show interfaces ethernet brief

Use this command to display brief information of interfaces, including interface status, output and input bandwidth usage, and the numbers of output and input packet errors.
show interfaces [*interface-type interface-number*] **ethernet brief [up | down]**

Parameter Description

Parameter	Description
interface-type interface-number	Specifies interface type and interface number. Information of all interfaces are displayed if this field is not specified.
up	Indicates connected interfaces.
down	Indicated disconnected interfaces.

Command Mode All CLI user modes

Default Level 14

Usage Guide If no interface is specified, information of all interfaces is displayed.
Physical ports, aggregation ports and management ports are supported.

Configuration Examples

The following example displays the brief information about Interface GigabitEthernet 0/1.

```
Hostname#show interfaces GigabitEthernet 0/1 ethernet brief

down: link down

*down: administratively down

disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)

Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage  Description
---------  ---------  ----  --------  -------  -------  -----------  ------------  -----------
Gi0/1       down       1     OFF       Unknown  Unknown  0.00%        0.00%         10G port
```

Note: If an interface is disabled, you can run the command to find out why it is error disabled. 0.01% is displayed when the usage is lower than 0.01% and there is network traffic working.

The following example displays the brief information about connected interfaces.

```
Hostname#show interfaces ethernet brief up

down: link down

*down: administratively down

disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)

Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage  Description
---------  ---------  ----  --------  -------  -------  -----------  ------------  -----------
Gi0/1        UP       1     OFF       Full     1000M    79.77%       79.77%        10G port
```

The following example displays the brief information of all interfaces.

```
Hostname#show interfaces ethernet brief

down: link down

*down: administratively down

disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)

Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage  Description
---------  ---------  ----  --------  -------  -------  -----------  ------------  -----------
```

```
Gi0/1        *down       1      OFF       Unknown   Unknown   0.00%        0.00%
10G port
Gi0/2         down       1      OFF       Unknown   Unknown   0.00%        0.00%
Gi0/3         down       1      OFF       Unknown   Unknown   0.00%        0.00%
Ag1           up         1      OFF       Full      1000M     46.78%       46.77%
Mg0           up       routed   --        Full      1000M      --          --
IP management Console
```

1.27 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the link state statistics of all interfaces are displayed.

Configuration Examples The following example displays the link state statistics of interface GigabitEthernet 0/1.

```
Hostname# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface    Link state    Link state change times     Last change time
-----------  ---------     -----------------------
-------------------
Gi 0/1       down          100                         2012-12-24
15:00:00
```

Interface	Description
Link state	Current link state.
Link state change times	The count of link state change.
Last change time	The time when the last link state change occurs.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.28 show interfaces status

Use this command to display interface status information.

show interfaces [*interface-type interface-number*] **status**

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.
status	Displays interface status information, including speed and duplex.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the status information of all interfaces is displayed.

Configuration Examples The following example displays the status information of interface GigabitEthernet 0/1.

```
Hostname#show interfaces GigabitEthernet 0/1 status
Interface            Status      Vlan    Duplex  Speed   Type
-------------------  ----------  ------  ------  ------  ------
GigabitEthernet 0/1    up          1       Full    1000M   copper
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.29 show interfaces status err-disable

Use this command to display the interface violation status.

show interfaces [*interface-type interface-number*] **status err-disable**

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) The interface type and ID.

Defaults

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, violation status of all interfaces is displayed.

Configuration Examples The following example displays the violation status of interface GigabitEthernet 0/1.

```
Hostname#show interface gigabitEthernet 0/1 status err-disabled
Interface                    Status         Reason
-------------------------------- ---------------- ----------------
GigabitEthernet 0/1            err-disabled    BPDU Guard
```

The violation status is displayed as **err-disabled**.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.30 show interfaces transceiver

Use this command to display transceiver information of the interface.

show interfaces [*interface-type interface-number*] **transceiver** [**alarm** | **diagnosis**]

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.

transceiver	Displays the transceiver information.
alarm	Displays the alarm message of the transceiver. If there is no alarm message, it is displayed as None.
diagnosis	Displays the diagnostic parameters of the transceiver.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the transceiver information of all interfaces is displayed.

Configuration Examples The following example displays the transceiver information of interface Gigabitethernet 5/4.

```
Hostname#show interfaces GigabitEthernet 5/4 transceiver
Transceiver Type    :  1000BASE-SX-SFP
Connector Type      :  LC
Wavelength(nm)      :  850
Transfer Distance   :
   50/125 um OM2 fiber
      -- 550m
   62.5/125 um OM1 fiber
      -- 270m
Digital Diagnostic Monitoring  : YES
Vendor Serial Number          : 101680093602489
```

The following example displays the alarm message of the transceiver of interface Gigabitethernet 5/4.

```
Hostname#show interfaces GigabitEthernet 5/4 transceiver alarm
gigabitEthernet 5/4 transceiver current alarm information:
RX  loss of signal
```

The following example displays the diagnostic parameters of the transceiver of interface Gigabitethernet 5/4.

```
Hostname#show interfaces GigabitEthernet 5/4 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)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.31 show interfaces usage

Use this command to display bandwidth usage of the interface.

show interfaces [*interface-type interface-number*] **usage** [*up* | *down*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) The interface type and ID.
up	(Optional) Displays the port up statistics.
down	(Optional) Displays the port down statistics.

Defaults N/A

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the *bandwidth* parameter configured on the interface.

Configuration Examples The following example displays bandwidth usage of interface GigabitEthernet 0/1.

```
Hostname#show interfaces GigabitEthernet 0/1 usage
Interface                 Bandwidth    Average Usage     Output Usage
Input Usage
----------------------------- ------------- ------------------
----------------- -----------------
GigabitEthernet 0/0         1000 Mbit    0.002822759%      0.001183280%
0.004462237%
```

Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.32 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.

shutdown

no shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the administrative status of an interface is Up.

Command Mode Interface configuration mode

Usage Guide Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

Configuration Examples The following example disables an interface.

```
Hostname(config)# interface aggregateport 1
Hostname(config-if)# shutdown
```

The following example enables an interface.

```
Hostname(config)# interface aggregateport 1
Hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear interface	Resets the hardware.
show interfaces	Displays the interface information.

Platform Description N/A

1.33 snmp trap link-status

Use this command to send LinkTrap on a port. Use the **no** form of this command to disable this function.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default

Command Mode Interface configuration mode.

Usage Guide For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Configuration Examples The following example disables the interface from sending LinkTrap on the interface.

```
Hostname(config)# interface gigabitEthernet 1/1
Hostname(config-if)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
Hostname(config)# interface gigabitEthernet 1/1
Hostname(config-if)# snmp trap link-status
```

Related Commands

Command	Description
snmp trap link-status	Enables the interface to send LinkTrap on the interface.
no snmp trap link-status	Disables the interface from sending LinkTrap on the interface.

Platform Description N/A

1.34 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

snmp-server if-index persist

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.

Configuration Examples The following example enables the interface index persistence.

```
Hostname(config)# snmp-server if-index persist
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.35 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

speed [**10 | 100 | 1000 || 2500 | auto**]

Parameter Description

Parameter	Description
10	The transmission rate of the interface is 10 Mbps.
100	The transmission rate of the interface is 100 Mbps.
1000	The transmission rate of the interface is 1000 Mbps.
2500	The transmission rate of the interface is 2.5 Gbps.
auto	Self-adaptive

Defaults The default is **auto**.

Command Mode Interface configuration mode.

Usage Guide If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

Configuration Examples The following example sets the speed on interface gigabitethernet 1/1 to 100Mbps.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# speed 100
```

Related Commands

Command	Description

show interfaces	Displays the interface information.

Platform Description N/A

1.36 switchport

Use this command to configure a Layer 3 interface. Use the **no** form of this command to restore the default setting.

switchport

no switchport

Parameter Description

Parameter	Description
N/A	N/A

Defaults All the interfaces are in Layer 2 mode by default.

Command Mode Interface configuration mode.

Usage Guide This command is valid only for physical interfaces. The **switchport** command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.

Configuration Examples The following example configures a Layer 3 interface.

```
Hostname(config-if)# switchport
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.37 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of this command to restore the default setting.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter Description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command Mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN.
If the port is a trunk port, the operation does not take effect.

Configuration Examples The following example configures interface gigabitethernet 1/1 as a statistic access port and adds it to VLAN 2.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Configures the interface as Layer 2 mode (switch port mode).
switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

1.38 switchport protected

Use this command to configure the interface as the protected port. Use the **no** form of this command to restore the default setting.
switchport protected
no switchport protected

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide The ports that are set as the protected ports cannot switch on L2, but can route on L3. A protected port can communicate with an unprotected port. Use the **show interfaces** command to display configuration.

Configuration Examples The following example configures interface gigabitethernet 1/1 as a protected port.

```
Hostname(config)#interface gigabitethernet 1/1
Hostname(config-if)# switchport protected
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

2 MAC Address Commands

2.1 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

clear mac-address-table dynamic [**address** *mac-addr* [**interface** *interface-id*] [**vlan** *vlan-id*] | { [**interface** *interface-id*] [**vlan** *vlan-id*] }]

Parameter Description

Parameter	Description
dynamic	Clears all the dynamic MAC addresses.
address *mac-addr*	Clears the specified dynamic MAC address.
interface *interface-id*	Clears all the dynamic MAC addresses of the specified interface.
vlan *vlan-id*	Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use the **show mac-address-table dynamic** command to display all the dynamic MAC addresses.

Configuration Examples The following command clears all the dynamic MAC addresses.

```
Hostname# clear mac-address-table dynamic
```

Related Commands

Command	Description
show mac-address-table dynamic	Displays dynamic MAC address.

Platform Description N/A

2.2 mac-address-learning

Use this command to enable the port address learning. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning

no mac-address-learning

default mac-address-learning

Parameter

Parameter	Description

Description	N/A	N/A

Defaults The address learning function is enabled.

Command Mode Interface configuration mode.

Usage Guide MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.

Configuration Examples The following example disables the port address learning function.

```
Hostname(config-if)# no mac-address-learning
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 mac-address-learning (global)

Use this command to enable MAC address learning globally. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning enable

Use this command to disable MAC address learning globally.

mac-address-learning disable

Use this command to restore MAC address learning globally.

default mac-address-learning

Parameter Description

Parameter	Description
enable	Enables MAC address learning globally.
disable	Disables MAC address learning globally.

Defaults The **mac-address-learning enable** command is enabled by default.

Command Mode Global configuration mode

Usage Guide When this function is enabled, the MAC address is learned in global configuration mode the same as learned in interface configuration mode.

Configuration Examples The following example disables MAC address learning globally.

```
Hostname(config)# mac-address-learning disable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.4 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** or **default** form of the command to restore the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

default mac-address-table aging-time

Parameter Description	Parameter	Description
	seconds	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.

Defaults The default is 300.

Command Mode Global configuration mode.

Usage Guide Use **show mac-address-table aging-time** to display configuration.

Configuration Examples The following example sets the aging time of the dynamic MAC address to 500 seconds.

```
Hostname(config)# mac-address-table aging-time 500
```

Related Commands	Command	Description
	show mac-address-table aging-time	Displays the aging time of the dynamic MAC address.
	show mac-address-table dynamic	Displays dynamic MAC address.

Platform Description N/A

2.5 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** or **default** form of the command to restore the default setting.

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

Parameter	Description
mac-address	Filtering Address
vlan-id	VLAN ID, in the range from 1 to 4094.

Defaults No filtering address is configured by default.

Command Mode Global configuration mode.

Usage Guide The filtering MAC address shall not be a multicast address.

Configuration Examples The following example configures the filtering MAC address for VLAN 1.

```
Hostname(config)#mac-address-table filtering 0000.0202.0303  vlan 3
```

Related Commands

Command	Description
clear mac-address-table filtering	Clears the filtering MAC address.

Platform Description N/A

2.6 mac-address-table notification

Use this command to enable the MAC address notification function. Use The **no** or **default** form of the command to restore the default setting.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

default mac-address-table notification [interval | history-size]

Parameter Description

Parameter	Description
interval *value*	Sets the interval of sending the MAC address trap message, 1 second by default.
history-size *value*	Sets the maximum number of the entries in the MAC address notification table, 50 entries by default.

Defaults By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

Command Mode Global configuration mode.

Usage Guide The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Configuration Examples The following example enables the MAC address notification function.

```
Hostname(config)# mac-address-table notification
Hostname(config)# mac-address-table notification interval 40
Hostname(config)# mac-address-table notification history-size 100
```

Related Commands

Command	Description
snmp-server enable traps	Sets the method of handling the MAC address trap message.
show mac-address-table notification	Displays the MAC address notification configuration and the MAC address trap notification table.
snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.

Platform Description N/A

2.7 mac-address-table static

Use this command to configure a static MAC address. Use the **no** or **default** form of the command to restore the default setting.

mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

default mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the specified entry
vlan-id	VLAN ID of the specified entry, in the range from 1 to 4094.
interface-id	Interface (physical interface or aggregate port) that packets are forwarded to

Defaults No static MAC address is configured by default.

Command Mode Global configuration mode.

Usage Guide A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use **show mac-address-table static** to display the static MAC address.

Configuration Examples

```
N/A
```

Related Commands

Command	Description
show mac-address-table static	Displays the static MAC address.

Platform Description N/A

2.8 max-dynamic-mac-count

Use this command to set the maximum number of MAC address learned dynamically on the VLAN or interface. Use the **no** or **default** form of this command to restore the default setting.

max-dynamic-mac-count *num*

no max-dynamic-mac-count

default max-dynamic-mac-count

Parameter Description

Parameter	Description
num	Sets the maximum number of MAC addresses.

Defaults The maximum number is not set by default.

Command Mode VLAN configuration mode / Interface configuration mode

Usage Guide This command is used to set the maximum number of MAC addresses learned dynamically on the VLAN or interface.

If the number of MAC addresses dynamically learned on the VLAN or interface reaches the upper limit, MAC address learning is disabled on the VLAN or interface.

If the number of MAC addresses reaches the upper limit when this command is configured, the surplus MAC addresses are not cleared. Instead, they remain and then age. MAC address learning is disabled on the VLAN or interface.

Use the **show mac-address-table max-dynamic-mac-count** command to display the maximum number of MAC addresses learned dynamically on the VLAN or interface.

Configuration Examples The following example sets the maximum number of MAC addresses dynamically learned on VLAN 1.

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#vlan 1
Hostname(config-vlan)#max-dynamic-mac-count 160
```

The following example sets the maximum number of MAC addresses dynamically learned on

interface GigabitEthernet 0/1.

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 160
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.9 show mac-address-learning

Use this command to display the MAC address learning.

show mac-address-learning

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode All modes.

Usage Guide N/A

Configuration Examples The following example displays the MAC address learning.

```
Hostname# show mac-address-learning
GigabitEthernet 0/0     learning ability: disable
GigabitEthernet 0/1     learning ability: enable
GigabitEthernet 0/2     learning ability: enable
GigabitEthernet 0/3     learning ability: enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.10 show mac-address-table

Use this command to display all types of MAC addresses (including dynamic address, static address

and filter address).

show mac-address-table [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
address *mac-addr*	The MAC address.
interface *interface-id*	The Interface ID.
vlan *vlan-id*	The VLAN ID, in the range from 1 to 4094.

Defaults N/A

Command Mode All modes

Usage Guide N/A

Configuration Examples The following example displays the MAC address.

```
Hostname# show mac-address-table address 00d0.f800.1001
Vlan       MAC Address         Type    Interface
-------    ------------      --------   --------
1          00d0.f800.1001      STATIC  GigabitEthernet 1/1
Hostname# show mac-address-table
Vlan       MAC Address         Type    Interface
-------    ------------      --------   --------
1          00d0.f800.1001      STATIC  GigabitEthernet 1/1
1          00d0.f800.1002      DYNAMIC GigabitEthernet 1/1
1          00d0.f800.1003      OTHER   GigabitEthernet 1/1
1          00d0.f800.1004      FILTER
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.11 show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

show mac-address-table aging-time

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode All modes.

Usage Guide N/A

Configuration Examples The following example displays the aging time of the dynamic MAC address.

```
Hostname# show mac-address-table aging-time
Aging time  : 300
```

Related Commands	Command	Description
	mac-address-table aging-time	Sets the aging time of the dynamic MAC address.

Platform Description N/A

2.12 show mac-address-table count

Use this command to display the number of address entries in the address table.

show mac-address-table count [**interface** *interface-id* **| vlan** *vlan-id*]

Parameter Description	Parameter	Description
	interface *interface-id*	Interface ID
	vlan *vlan-id*	VLAN ID, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.

The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.

The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

Configuration Examples The following example displays the number of MAC address entries.

```
Hostname# show mac-address-table count
Dynamic Address Count : 51
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses  : 51
Total Mac Address Space Available: 8139
```

The following example displays the number of MAC address in VLAN 1.

```
Hostname# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 7
```

The following example displays the number of MAC addresses on interface g0/1.

```
Hostname# show mac-address-table interface g0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 10
```

Related Commands

Command	Description
show mac-address-table static	Displays the static address.
show mac-address-table filtering	Displays the filtering address.
show mac-address-table dynamic	Displays the dynamic address.
show mac-address-table address	Displays all the address information of the specified address.
show mac-address-table interface	Displays all the address information of the specified interface.
show mac-address-table vlan	Displays all the address information of the specified vlan.

Platform Description N/A

2.13 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

show mac-address-table dynamic [**address** *mac-add r*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN of the entry, in the range from 1 to 4094.
interface-id	Interface that the packet is forwarded to.

	It may be a physical port or an aggregate port

Defaults

Command Mode All modes.

Usage Guide N/A

Configuration Examples The following example displays the dynamic MAC address.

```
Hostname# show mac-address-table dynamic
Vlan   MAC Address     Type   Interface
------------------------ -------- ------------------
1   0000.0000.0001    DYNAMIC gigabitethernet 1/1
1   0001.960c.a740    DYNAMIC gigabitethernet 1/1
1   0007.95c7.dff9    DYNAMIC gigabitethernet 1/1
1   0007.95cf.eee0    DYNAMIC gigabitethernet 1/1
1   0007.95cf.f41f    DYNAMIC gigabitethernet 1/1
1   0009.b715.d400    DYNAMIC gigabitethernet 1/1
1   0050.bade.63c4    DYNAMIC gigabitethernet 1/1
```

Related Commands

Command	Description
clear mac-address-table dynamic	Clears the dynamic MAC address.

Platform Description N/A

2.14 show mac-address-table filtering

Use this command to display the filtering MAC address.

show mac-address-table filtering [**ddr** *mac-addr*] [**vlan** *vlan-Id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the filtering MAC address.

```
Hostname# show mac-address-table filtering
Vlan    MAC Address    Type   Interface
------- ----------------- ------- -----------
 1    0000.2222.2222   FILTER Not available
```

Related Commands	Command	Description
	mac-address-table filtering	Configures the filtering MAC address.

Platform Description N/A

2.15 show mac-address-table interface

Use this command to display all the MAC addresses on the specified interface including static and dynamic MAC address

show mac-address-table interface [*interface-id*] [**vlan** *vlan-id*]

Parameter Description	Parameter	Description
	interface-id	Displays the MAC address information of the specified Interface (physical interface or aggregate port).
	vlan-id	VLAN ID of the entry, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all the MAC addresses on interface gigabitethernet 1/1.

```
Hostname# show mac-address-table interface
gigabitethernet 1/1
Vlan  MAC Address  Type   Interface
----- ------------- -------- ----------------
1   00d0.f800.1001 STATIC  gigabitethernet 1/1
1   00d0.f800.1002 STATIC  gigabitethernet 1/1
1   00d0.f800.1003 STATIC  gigabitethernet 1/1
1   00d0.f800.1004 STATIC  gigabitethernet 1/1
```

Related Commands	Command	Description
	show mac-address-table static	Displays the static MAC address.
	show mac-address-table filtering	Displays the filtering MAC address.

show mac-address-table dynamic	Displays the dynamic MAC address.
show mac-address-table address	Displays all types of MAC addresses.
show mac-address-table vlan	Displays all types of MAC addresses of the specified VLAN.
show mac-address-table count	Displays the address counts in the MAC address table.

Platform Description N/A

2.16 show mac-address-table max-dynamic-mac-count

Use this command to display the maximum number of dynamic MAC addresses learned on the VLAN or interface.

show mac-address-table max-dynamic-mac-count { **vlan** [*vlan-id*] | **interface** [*interface-id*] }

Parameter Description

Parameter	Description
vlan	Displays the dynamic MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC address learning.
vlan-id	Displays the dynamic MAC address learned on the specified VLAN.
interface	Displays the dynamic MAC address learned on all interfaces which are configured with the maximum number of dynamic MAC address learning.
interface-id	Displays the dynamic MAC address learned on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC addresses.

```
Hostname#show mac-address-table max-dynamic-mac-count vlan
Vlan Limit   MAC count Learning
---- ------- --------- --------
1    160       6        YES
```

The following example displays the MAC address learned dynamically on the specified VLAN.

```
Hostname#show mac-address-table max-dynamic-mac-count vlan 1
Vlan Limit   MAC count Learning
---- ------- --------- --------
```

```
1    160        6         YES
```

Field	Description
Vlan	The VLAN ID.
Limit	The maximum number of MAC addresses.
MAC count	The number of MAC address learned dynamically on the VLAN.
Learning	Whether MAC address learning is disabled on the VLAN.

The following example displays the MAC address learned on all interfaces which are configured with the maximum number of the dynamic MAC address.

```
Hostname#show mac-address-table max-dynamic-mac-count interface
Interface              Limit   MAC count Learning
---------------------- ------- --------- --------
GigabitEthernet 0/1     160     6         YES
```

The following example displays the MAC address learned dynamically on the specified interface.

```
Hostname#show mac-address-table max-dynamic-mac-count interface
GigabitEthernet 0/1
Interface              Limit   MAC count Learning
---------------------- ------- --------- --------
GigabitEthernet 0/1     160     6         YES
```

Field	Description
Interface	The Interface ID
Limit	The maximum number of MAC addresses.
MAC count	The number of MAC address learned dynamically on the interface.
Learning	Whether MAC address learning is disabled on the interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 show mac-address-table notification

Use this command to display the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [**interface** [*interface-id*] | **history**]

Parameter Description

Parameter	Description
interface	Displays the MAC address notification configuration on all interfaces.

interface *interface-id*	Displays the MAC address notification configuration on a specific interface.
history	Displays the MAC address notification history.

Defaults

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the MAC address notification configuration globally.

```
Hostname#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Related Commands

Command	Description
mac-address-table notification	Enables MAC address notification.
snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.

Platform Description N/A

2.18 show mac-address-table static

Use this command to display the static MAC address.

show mac-address-table static [**addr** *mac-add r*] [**interface** *interface-Id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry, within the range from 1 to 4094.
interface-id	Interface of the entry physical interface or aggregate port

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the static MAC addresses

```
Hostname# show mac-address-table static
Vlan    MAC Address     Type   Interface
---------- ------------------- -------- ---------
1  00d0.f800.1001  STATIC  gigabitethernet 1/1
1  00d0.f800.1002  STATIC  gigabitethernet 1/1
1  00d0.f800.1003  STATIC  gigabitethernet 1/1
```

Related Commands

Command	Description
mac-address-table static	Configures the static MAC address.

Platform Description N/A

2.19 show mac-address-table vlan

Use this command to display all addresses of the specified VLAN.

show mac-address-table vlan [*vlan-id*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID of the entry, within the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all addresses of the specified VLAN.

```
Hostname# show mac-address-table vlan 1
Vlan  MAC Address    Type    Interface
----- -------------  ------- ------------------
1   00d0.f800.1001  STATIC  gigabitethernet 1/1
1   00d0.f800.1002  STATIC  gigabitethernet 1/1
1   00d0.f800.1003  STATIC  gigabitethernet 1/1
```

Related Commands

Command	Description
show mac-address-table static	Displays static addresses.
show mac-address-table filtering	Displays filtered addresses.
show mac-address-table dynamic	Displays dynamic addresses.
show mac-address-table address	Displays all address information about the specified address.

show mac-address-table interface	Displays all address information about the specified interface.
show mac-address-table count	Displays the number of addresses in the address table.

Platform Description N/A

2.20 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. Use The **no** or **default** form of the command to restore the default setting.

snmp trap mac-notification { **added** | **removed** }

no snmp trap mac-notification { **added** | **removed** }

default snmp trap mac-notification { added | removed }

Parameter Description

Parameter	Description
added	Notifies when a MAC address is added.
removed	Notifies when a MAC address is removed

Defaults

Command Mode Interface configuration mode.

Usage Guide Use **show mac-address-table notification interface** to display configuration.

Configuration Examples The following example enables the MAC address trap notification on interface gigabitethernet 1/1.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# snmp trap mac-notification added
```

Related Commands

Command	Description
mac-address-table notification	Enables MAC address notification.
show mac-address-table notification	Displays the MAC address notification configuration and the MAC address notification table.

Platform Description N/A

3 Aggregate Port Commands

3.1 aggregateport load-balance

Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the **no** form of this command to return the default setting.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** }

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.

Defaults Load balancing can be based on source and destination MAC addresses, source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing (applicable to switches with CB line cards).

Command Mode Global configuration mode/Interface configuration mode

Usage Guide You can run aggregateport load-balance in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run no aggregateport load-balance in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.

Configuration Examples The following example configures a load-balance algorithm globally based on the destination MAC address.

```
Hostname(config)# aggregateport load-balance dst-mac
```

Related Commands

Command	Description
show aggregateport load-balance	Displays aggregate port configuration.

Platform Description N/A

3.2 aggregateport member linktrap

Use this command to send LinkTrap to aggregate port members. Use the **no** form of this command to restore the default setting.

aggregateport member linktrap

no aggregateport member linktrap

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function cannot be enabled by running the **snmp trap link-status** command in interface configuration mode. However, it can be enabled by running the **aggregateport member linktrap** command in global configuration mode.

Configuration Examples The following example enables the LinkTrap function on the aggregate port members.

```
Hostname# configure terminal
Hostname(config)# aggregateport member linktrap
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 interfaces aggregateport

Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the **no** form of this command to restore the default setting.

interfaces aggregateport *ap-number*

no interfaces aggregateport *ap-number*

Parameter Description

Parameter	Description
ap-number	Aggregate port number.

Defaults The aggregate port is not created by default.

Command Mode Global configuration mode

Usage Guide If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.

Configuration Examples The following example creates AP 5 and enters its interface configuration mode.

```
Hostname# configure terminal
Hostname(config)# interfaces aggregateport 5
Hostname(config-if-Aggregateport 5)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 lacp port-priority

Use this command to set the priority of the LACP AP member port. Use the **no** form of this command to restore the default setting.

lacp port-priority *port-priority*

no lacp port-priority

Parameter Description

Parameter	Description
port-priority	The LACP port priority, in the range from 0 to 65535.

Defaults The default is 32768.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples This example sets the LACP port priority of interface Gi0/1 to 4096.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lacp port-priority 4096
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 lacp short-timeout

Use this command to configure the short-timeout mode for the LACP AP member port. Use the no form of this command to restore the default setting.

lacp short-timeout

no lacp short-timeout

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is long-timeout mode.

Command Mode Interface configuration mode

Usage Guide In long-timeout mode, the port sends an LACP packet every 30 seconds. If the packet is not received in 90 seconds, the connection times out.

In short-timeout mode, the port sends an LACP packet every 1 second. If the packet is not received in 3 seconds, the connection times out.

Configuration Examples The following example configures the short-timeout mode for the LACP AP member port.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lacp short-timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 lacp system-priority

Use this command to set the LACP system priority. Use the **no** form of this command to restore the default setting.

lacp system-priority *system-priority*

no lacp system-priority

Parameter Description

Parameter	Description
system-priority	The LACP system priority, in the range from 0 to 65535.

Defaults The default is 32768.

Command Mode Global configuration mode.

Usage Guide

Configuration Examples The following example sets the LACP system priority to 4096.

```
Hostname(config)# lacp system-priority 4096
```

Related Commands

Command	Description
port-group *key* **mode** { **active** | **passive** }	Enables the LACP on the port and specifies the aggregation group ID and operation mode.
lacp port-priority	Sets the LACP port priority.

Platform Description N/A

3.7 port-group

Use this command to assign a physical interface to be a member port of a static aggregate port or an LACP aggregate port. Use the **no** form of this command to restore the default setting.

port-group *port-group-number*
port-group *key-number* **mode** { **active** | **passive** }
no port-group

Parameter Description

Parameter	Description
port-group-number	Member group ID of an aggregate port, the interface number of the aggregate port.
key-number	Member group ID of an LACP aggregate port, the interface number of the LACP aggregate port.
active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Defaults By default, the physical port does not belong to any aggregate port.

Command Mode Interface configuration mode.

Usage Guide All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Configuration Examples The following example specifies the Ethernet interface 1/3 as a member of the static AP 3.

```
Hostname(config)# interface gigabitethernet 1/3
Hostname(config-if-GigabitEthernet 1/3)# port-group 3
```

The following example specifies the Ethernet interface 2/3 as a member of the LACP AP4 and set the aggregation mode to active.

```
Hostname(config)# interface gigabitethernet 2/3
Hostname(config-if-GigabitEthernet 2/3)# port-group 4 mode active
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 show aggregateport

Use this command to display the aggregate port configuration.
show aggregateport { [*aggregate-port-number*] **summary** | **load-balance** }

Parameter Description

Parameter	Description
aggregate-port-number	Number of the aggregate port.

load-balance	Displays the load-balance algorithm on the aggregate port.
summary	Displays the summary of the aggregate port.

Defaults N/A

Command Mode Any mode

Usage Guide If the aggregate port number is not specified, all the aggregate port information will be displayed.

Configuration Examples The following example displays the aggregate port configuration.

```
Hostname# show aggregateport 1 summary
AggregatePort  MaxPorts        SwitchPort Mode    Load balance                Ports
-------------  ---------------- ---------- ------  --------------------------
------------------------
Ag1            8                Enabled    ACCESS  dst-mac                     Gi0/2
```

Note:

If the system does not support load-balancing mode based on aggregate port, then **Load balance** field will not be displayed.

Related Commands

Command	Description
aggregateport load-balance	Configures a load-balance algorithm of AP.

Platform Description N/A

3.9 show lacp summary

Use this command to display the LACP aggregation information.

show lacp summary [*key*]

Parameter Description

Parameter	Description
key	Specifies the aggregation group id to show. If it is not specified, all aggregation group information is displayed by default.

Defaults N/A

Command Mode Any mode.

Usage Guide N/A

Configuration Examples The following example displays the LACP aggregation information.

```
Hostname(config)# show lacp summary 3
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 3:
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
```

Field	Description
Local information	Displays the local LACP information.
Port	Displays the system port ID.
Flags	Displays the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.
State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “susp” indicates that the port is not aggregated.
LACP Port Priority	Displays the LACP port priority.
Oper Key	Displays the port operation key.
Port Number	Displays the port number.
Port State	Displays the flag bit for the LACP port state.
Partner information	Partly Displays the LACP information of the peer port.
Dev ID	Partly Displays the system MAC information of the peer device.

Related Commands

Command	Description
port-group *key* **mode**	Enables the LACP on the port and specifies the aggregation group ID and operation mode.

Platform Description N/A

4 VLAN Commands

4.1 add

Use this command to add one or a group Access interface into current VLAN. Use the **no** or **default** form of the command to remove the Access interface.

add interface { *interface-id* | **range** *interface-range* }

no add interface { *interface-id* | **range** *interface-range* }

default add interface { *interface-id* | **range** *interface-range* }

Parameter Description

Parameter	Description
interface-id	Layer-2 Ethernet interface or layer-2 AP port.
range *interface-range*	Range of the Layer-2 Ethernet interface or layer-2 AP port.

Defaults All layer-2 Ethernet interfaces are in the VLAN1.

Command mode VLAN configuration mode.

Usage Guide This command is only valid for the access port.

The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** *vlan-id* command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.

The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Configuration Examples The following example adds the interface GigabitEthernet 0/10 to VLAN20.

```
Hostname# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
Hostname# 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 the interface range GigabitEthernet 0/1-10 to VLAN200.

```
Hostname# configure terminal
SwitchA(config)#vlan 200
SwitchA(config-vlan)#add interface range GigabitEthernet 0/1-10
Hostname# show vlan
```

```
SwitchA#show vlan
VLAN Name        Status                    Ports
---- -------    ------------    ----------------------------
1 VLAN0001    STATIC   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
200 VLAN0200 STATIC  Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5,
Gi0/6,Gi0/7,Gi0/8,Gi0/9,Gi0/10
```

The following example adds the AggregatePort10 to VLAN20.

```
Hostname# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10
Hostname# show interface aggregateport 10 switchport
Interface  Switchport   Mode  Access  Native Protected  VLAN lists
----------  --------      -----  -----  ---- ---------- -------
AggregatePort 10 enabled  ACCESS  20   1   Disabled  ALL
```

Related Commands

Command	Description
show interface *interface-id* **switchport**	Displays the layer-2 interfaces.

Platform Description N/A

4.2 name

Use this command to specify the name of a VLAN. Use the **no** or **default** form of this command to restore the default setting.

name *vlan-name*

no name

default name

Parameter Description

Parameter	Description
vlan-name	VLAN name

Defaults The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

Command mode VLAN configuration Mode.

Usage Guide N/A

Configuration Examples The following example sets the name of VLAN to 10.

```
Hostname(config)# vlan 10
Hostname(config-vlan)# name vlan10
```

Related Commands

Command	Description
show vlan	Displays member ports of the VLAN.

Platform Description N/A

4.3 show vlan

Use this command to display member ports of the VLAN.

show vlan [**id** *vlan-id*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults N/A

Command mode All modes

Usage Guide N/A

Configuration Examples The following command displays the status of VLAN 1.

```
Hostname(config-vlan)#show vlan id 20
VLAN Name                            Status    Ports
---- -------------------------------- ---------
-----------------------------------
  20 VLAN0020                         STATIC    Gi0/1
```

The following command displays the status 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 VLAN0002                      STATIC    Gi0/1
20 VLAN0020                        STATIC    Gi0/1
```

Related Commands

Command	Description
name	VLAN name.
switchport access	Adds the interface to a VLAN.

Platform Description N/A

4.4 switchport access

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** or **default** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

default switchport access vlan

Parameter Description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN.
If the port is a trunk port, the operation does not take effect.

Configuration Examples

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Specifies the interface as Layer 2 mode (switch port mode).
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

4.5 switchport hybrid allowed

Use this command to add the port to the VLAN or remove the port from the VLAN, Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid allowed vlan { { [**add** | **only**] **tagged** *vlist* | [**add**] **untagged** *vlist* } | **remove** *vlist* }

no switchport hybrid allowed vlan

default switchport hybrid allowed vlan

Parameter Description

Parameter	Description
add	Adds the port to the VLAN.
only	Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list.
tagged	Adds the port to the VLAN and the VLAN packets going out on the port are tagged with VLAN ID.
untagged	Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID.
remove	Removes the port from the VLAN.
vlist	Specifies the VLAN.

Defaults By default, the hybrid port is in all VLANs. All VLAN packets (except native VLAN packets) going out on the port are tagged with VLAN ID. Native VLAN packets are not tagged with VLAN ID.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example adds the hybrid port to VLAN 20 and VLAN 30 and the VLAN packets going out on the port are not tagged with VLAN ID.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid
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 the hybrid port to VLAN 40 and VLAN 50 and the VLAN packets going out on the port are tagged with VLAN ID,

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#switchport mode hybrid
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 removes the hybrid port from VLAN 20.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan remove 20
```

The following example adds the hybrid port to VLAN 20 and deletes all the other VLANs. The VLAN packets going out on the port are tagged with VLAN ID.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan only tagged 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 switchport hybrid native

Use this command to configure the native VLAN for the hybrid port. Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid native vlan *vlan-id*

no switchport hybrid native vlan

default switchport hybrid native vlan

Parameter Description

Parameter	Description
vlan-id	Configures the native VLAN for the hybrid port.

Defaults The default is VLAN 1.

Command mode Interface configuration mode

Usage Guide Native VLAN packets going out on the hybrid port are not tagged with VLAN ID. Packets not tagged with VLAN ID coming in on the hybrid port are taken as native VLAN packets.

Configuration Examples The following example configures VLAN 20 as the native VLAN for hybrid port GigabitEthernet 0/1.

```
Hostname(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Hostname(config-if-GigabitEthernet 0/1)#switchport hybrid native vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or a servicechain port. Use the **no** or **default** form of this command to restore the default setting.

switchport mode { **access** | **trunk** | **hybrid** | **uplink** }

no switchport mode

default switchport mode

Parameter Description

Parameter	Description
access	Configures the switch port as an access port.
trunk	Configures the switch port as a trunk port.
hybrid	Configures the switch port as a hybrid port.
uplink	Configures the switch port as an uplink port.

Defaults By default, the switch port is an access port.

Command mode Interface configuration mode.

Usage Guide If a switch port is an access port, the port can be added only to one VLAN. You can run the **switchport access vlan** command to specify the VLAN to which the port belongs.

If a switch port is a trunk port, the port is added to all VLANs by default. You can also run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.

If a switch port is an uplink port, the port is added to all VLANs by default. Different from the trunk port, the uplink port sends packets with a tag carried, that is, the tag of packets from default VLANs

will not be deleted. You can run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.
If a switch port is a hybrid port, the port is added to all VLANs by default. Different from a trunk port, a hybrid port can be added to a VLAN in tag or untag mode by running the **switchport hybrid allowed** command.

Configuration Examples

The following example configures port 1 as an access port.

```
Hostname(config)#int g 0/1
Hostname(config-if-GigabitEthernet 0/1)#switchport mode access
```

The following example configures port 1 as a trunk port.

```
Hostname(config)#int g 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

The following example configures port 1 as an uplink port.

```
Hostname(config)#int g 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode uplink
```

The following example configures port 1 as a hybrid port.

```
Hostname(config)#int g 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

Related Commands

Command	Description
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description

N/A

4.8 switchport trunk allowed vlan

Use this command to add the trunk/uplink port to the VLAN or remove a trunk/uplink port from the VLAN. Use the **no** or **default** form of the command to restore the default setting.
switchport trunk allowed vlan { **all** | { **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **only** *vlan-list* } }
no switchport trunk allowed vlan
default switchport trunk allowed vlan

Parameter Description

Parameter	Description
all	Adds the trunk/uplink port to all VLANs.
add	Adds the trunk/uplink port to the VLAN.

remove	Removes the trunk/uplink port from the VLAN port.
except	Removes the trunk/uplink port from the VLAN and adds the port to all the other VLANs.
only	Adds the trunk/uplink port to the specified VLAN and removes the port from the VLANs not on the VLAN list.
vlan-list	Specifies the VLAN.

Defaults The trunk/unlink port is in all VLANs by default.

Command mode Interface configuration mode.

Usage Guide A trunk/uplink port transmits all VLAN (1-4094) data by default. You can block some VLAN data by configuring this command. Use the **show interfaces** command to display configuration.

Configuration Examples The following example removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
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 removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
Hostname(config)# interface gigabitEthernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan
except 10
```

The following example removes uplink port GigabitEthernet 0/10 from VLAN 10.

```
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 uplink port GigabitEthernet 0/10 to all VLANs except VLAN10.

```
Hostname(config)# interface gigabitEthernet 0/10
Hostname(config-if-GigabitEthernet 0/10)# switchport trunk allowed
vlan except 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 switchport trunk native vlan

Use this command to configure the native VLAN for the trunk/uplink port. Use the **no** or **default** form of this command to restore the default setting.

switchport trunk native vlan *vlan-id*
no switchport trunk native vlan
default switchport trunk native vlan

Parameter Description

Parameter	Description
vlan-id	Native VLAN ID.

Defaults By default, the native VLAN for the trunk/uplink port is VLAN 1.

Command mode Interface configuration mode

Usage Guide After this function is enabled, packets not tagged with VLAN ID are taken as native VLAN packets. Tags are removed from native VLAN packets going out on the trunk port.

Configuration Examples The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/10.

```
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 VLAN 10 as the native VLAN for unlink port GigabitEthernet 0/10.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.10 vlan

Use this command to enter the VLAN configuration mode. Use the **no** or **default** form of this command to restore the default setting.

vlan { *vlan-id* | **range** *vlan-range* }
no vlan { *vlan-id* | **range** *vlan-range* }

default vlan { *vlan-id* | **range** *vlan-range* }

Parameter Description

Parameter	Description
vlan-id	VLAN ID Default VLAN (VLAN 1) cannot be removed.
vlan-range	VLAN ID range.

Defaults The default is static VLAN.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example creates VLAN 10.

```
Hostname(config)# vlan 10
Hostname(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays member ports of the VLAN.

Platform Description N/A

5 Voice VLAN Commands

5.1 show voice vlan

Use this command to display the Voice VLAN configurations and the current state, including the working mode of the port with Voice VLAN enabled.

show voice vlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the Voice VLAN configurations and the current state.

```
Hostname(config)# show voice vlan
Voice VLAN status: ENABLE            //Voice VLAN is enabled
Voice VLAN ID: 2                     //Voice VLAN ID
Voice VLAN security mode: Security   //Security Mode
Voice VLAN aging time: 5 minutes    //Aging Time
Voice VLAN cos: 6                   //Voice VLAN CoS
Voice VLAN dscp: 46                //Voice VLAN DSCP
Current voice vlan enabled port mode: // Voice VLAN  Enabled Port & Mode
PORT                    MODE
-------------------------------------------------
Fa0/1                   Auto
```

Related Commands

Command	Description
voice vlan *vlan-id*	Set a voice vlan.
voice vlan aging *minutes*	Set the Voice VLAN aging time.
voice vlan cos *cos-value*	Set the CoS value for the Voice VLAN.
voice vlan dscp *dscp-value*	Set the DSCP value for the Voice VLAN.
voice vlan enable	Enable the Voice VLAN.
voice vlan mode auto	Set the Voice VLAN working mode.
voice vlan security enable	Enable the Voice VLAN security mode.

Platform Description N/A

5.2 show voice vlan oui

Use this command to display the OUI address, OUI mask and the description information.

show voice vlan oui

Parameter Description

Parameter	Description
N/A	N/A

Defaults All modes.

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the OUI address.

```
Hostname(config)# show voice vlan oui
OUI             Mask             Description
--------------- ---------------- ---------------
0001.e300.0000  ffff.ff00.0000  Siemens phone
0003.6b00.0000  ffff.ff00.0000  Cisco phone
0004.0d00.0000  ffff.ff00.0000  Avaya phone
0060.b900.0000  ffff.ff00.0000  Philips/NEC phone
00d0.1e00.0000  ffff.ff00.0000  Pingtel phone
00e0.7500.0000  ffff.ff00.0000  Polycom phone
00e0.bb00.0000  ffff.ff00.0000  3com phone
```

The following lists the field description .

Field	Description
OUI	The OUI address, the source MAC address for the voice packet.
Mask	The OUI mask. The valid length for the OUI address.
Description	The description information for the OUI address.

Related Commands

Command	Description
voice vlan mac-address *mac-addr* **mask** *oui-mask* [**description** *text*]	Set the OUI address for the voice packet recognized by the Voice VLAN.

Platform Description N/A

5.3 voice vlan

Use this command to enable Voice VLAN in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan *vlan-id*

no voice vlan

Parameter Description

Parameter	Description
vlan-id	The Voice VLAN ID.

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide Use this command to enable the Voice VLAN and specify the Voice VLAN ID.

1. The corresponding VLAN shall be created before configuring the Voice VLAN;
2. The default VLAN is VLAN1 and cannot be set as the Voice VLAN;
3. A VLAN is not allowed to be set as the Voice VLAN and the Super VLAN at the same time;
4. With 802.1x VLAN auto-switching function enabled, the assigned VID shall not be set as the Voice VLAN ID;
5. RSPAN Remote VLAN and Voice VLAN cannot be the same VLAN, or it influences the remote port mirror and the Voice VLAN function.

Configuration Examples The following example sets the VLAN2 as the Voice VLAN.

```
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# voice vlan 2
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.4 voice vlan aging

Use this command to set the Voice VLAN aging time in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan aging *minutes*

no voice vlan aging

Parameter Description

Parameter	Description
minutes	The Voice VLAN aging time. Range: 5 to 10,000. Unit: minute.

Defaults The default is 1440 minutes.

Command mode Global configuration mode

Usage Guide If the device has not received any voice packets from the port within the aging time, this Voice VLAN will be removed from this port.

The aging time is valid for the auto-mode only.

Configuration Examples The following example sets the Voice VLAN aging time to 10 minutes.

```
Hostname(config)# voice vlan aging 10
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.5 voice vlan cos

Use this command to set the Voice VLAN CoS value in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan cos *cos-value*

no voice vlan cos

Parameter Description

Parameter	Description
cos-value	The Voice VLAN CoS value. Range: 0 to 7.

Defaults The default is 6.

Command mode Global configuration mode

Usage Guide You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DSCP value.

Configuration Examples The following example sets the Voice VLAN CoS value to 5.

```
Hostname(config)# voice vlan cos 5
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.6 voice vlan dscp

Use this command to set the Voice VLAN DSCP value in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameter Description

Parameter	Description
dscp-value	The Voice VLAN DSCP value. Range: 0 to 63.

Defaults The default is 46.

Command mode Global configuration mode

Usage Guide You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DHCP value.

Configuration Examples The following example sets the Voice VLAN DSCP value to 40.

```
Hostname(config)# voice vlan dscp 40
```

Related Commands

Command	Description

show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.7 voice vlan enable

Use this command to enable the Voice VLAN DSCP value in the interface configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan enable

no voice vlan enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide Use this command to enable the Voice VLAN on the physical port only. The Voice VLAN can be enabled on the Access Port, Trunk Port, Hybrid Port, Private VLAN host port, Private VLAN promiscuous port and Uplink port on the products.

With the global Voice VLAN disabled, although the Voice VLAN can be enabled on the port, it is invalid.

Configuration Examples The following example enables the Voice VLAN function on the interface FastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# voice vlan enable
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.8 voice vlan mac-address

Use this command to set the recognizable Voice VLAN OUI address. Use the **no** form of this command to restore the default setting.

voice vlan mac-address *mac-addr* **mask** *oui-mask* [**description** *text*]

no voice vlan mac-address *mac-addr*

Parameter Description

Parameter	Description
mac-addr	In the format of *H.H.H.* The source MAC address for the voice packets.
oui-mask	In the format of *H.H.H.* The valid length for the OUI address.
text	The description for the OUI address.

Defaults By default, no OUI has been configured.

Command mode Global configuration mode

Usage Guide Use this command to identify the voice packets from different vendors. The first three bytes of the MAC address for the voice device are used to identify the manufacture. Voice VLAN determines whether the packets are voice packets or not through the OUI address obtained from the source MAC address and the OUI mask for the received packets.

The Voice VLAN OUI address cannot be the multicast address and the configured mask shall be continuous.

Configuration Examples The following example sets the OUI address 0012.3400.0000 as the valid address for the Voice VLAN.

```
Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company A
```

Related Commands

Command	Description
show voice vlan oui	Display the OUI address, OUI address mask and the descriptions.

Platform Description N/A

5.9 voice vlan mode auto

Use this command to set the Voice VLAN auto mode. Use the **no** form of this command to disable

this function.

voice vlan mode auto

no voice vlan mode auto

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is in auto mode by default.

Command mode Interface configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

⚠ 1. With the Voice VLAN enabled on the port and in the manual mode, this port must be added to the Voice VLAN manually to ensure the function validity.

⚠ 2. When the port works in the auto-mode, to ensure normal functioning, the native VLAN of the port cannot be set as the Voice VLAN.

⚠ 3. The Trunk Port/Hybrid Port on the product can transmit the packets in all VLANs by default. First remove the Voice VLAN from the allowed VLAN list for the port, then enable the Voice VLAN to ensure that the port disconnecting with the voice device cannot be added to the Voice VLAN, or the port not used for a long time can be still in the Voice VLAN.

ℹ 1. With the Voice VLAN enabled on the port, the auto and manual modes switchover is disallowed. Disable the Voice VLAN first if it is necessary to switch the modes.

ℹ 2. In the auto mode, it fails to add/remove the port to/from the Voice Vlan by using the command.

Configuration Examples The following example sets the Voice VLAN on the interface FastEthernet 0/1 to work in the auto mode.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-vlan)# voice vlan mode auto
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

5.10 voice vlan security enable

Use this command to enable the Voice VLAN security mode in the global configuration mode. Use the **no** form of this command to disable this function.

voice vlan security enable

no voice vlan security enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command mode Global configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.


You are not recommended to transmit the voice and service data in the Voice VLAN at the same time. But if it is necessary for you, you shall ensure that the Voice VLAN security mode has been disabled.


In the security mode, only the source MAC addresses for the untagged packets and the packets carried with Voice VLAN tag are checked. For other packets carried with non-voice vlan tag that free from the Voice VLAN security/normal mode, the devices forward or discard those packets according to the VLAN rule.

Configuration Examples The following example enables the Voice VLAN security mode.

```
Hostname(config)# voice vlan security enable
```

Related Commands

Command	Description
show voice vlan	Display Voice VLAN configurations and the current state.

Platform N/A

Description

6 MSTP Commands

6.1 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to restore the default setting.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter Description

Parameter	Description
H.H.H	Indicates that only the BPDU messages from this MAC address are received.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide BPDU source MAC address check prevents BPDU packets from maliciously attacking the device and causing MSTP abnormality. When the device connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer device and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Configuration Examples The following example indicates only the BPDU with 00d0.f800.1e2f as the source MAC address will be received by interface Gi 1/1.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id-interface-id)# bpdu src-mac-check
00d0.f800.1e2f
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.2 bridge-frame forwarding protocol bpdu

Use this command to enable BPDU transparent transmission. Use the **no** form of this command to restore the default setting.

bridge-frame forwarding protocol bpdu
no bridge-frame forwarding protocol bpdu

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide In the IEEE 802.1Q standard, 01-80-C2-00-00-00, the destination MAC address of BPDU frames, is reserved. Devices following the IEEE 802.1Q standard don't forward BPDU frames. In real network deployment, devices may be required to support BPDU transparent transmission. For example, when a device is not enabled with STP, BPDU transparent transmission can help implement STP calculation.
BPDU transparent transmission works only when STP is disabled.

Configuration Examples The following example enables BPDU transparent transmission.

```
Hostname(config)# bridge-frame forwarding protocol bpdu
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.3 clear spanning-tree counters

Use this command to clear the statistics of the sent and received STP packets.
clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide It is used to clear the statistics of the sent and received STP packets.

Configuration Examples The following example clears the statistics of the sent and received STP packets.

```
Hostname# clear spanning-tree counters
```

The following example clears the statistics of the sent and received packets on interface Gi 0/1.

```
Hostname# clear spanning-tree counters interface gigabitethernet 0/1
```

Related Commands

Command	Description
show spanning-tree counters	Displays the statistics of STP transceived packets.

Platform Description N/A

6.4 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to force the interface to send the RSTP BPDU message.

Configuration Examples Forces to check the version of all interfaces.

```
Hostname# clear spanning-tree detected-protocols
```

Related

Command	Description

Commands		
	show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

clear spanning-tree mst *instance-id* **topochange record**

Parameter Description

Parameter	Description
instance-id	Instance ID. For STP and RSTP protocols, only instance 0 is valid.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears STP topology change record.

```
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   GI0/6              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.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.6 instance instance-id vlan vlan-range

Use this command to set instance and VLAN mapping relations. Use the **no** form of the command to

restore the default setting.

instance *instance-id* **vlan** *vlan-range*

no instance *instance-id* { **vlan** *vlan-range* }

Parameter Description

Parameter	Description
instance-id	Instance ID, in the range from 0 to 64
vlan-range	VLAN range, in the range from 1 to 4094.

Defaults

The default is instance 0.

Command Mode

MST configuration mode

Usage Guide

instance *instance-id* **vlan** *vlan-range*: Add VLAN to MST instance. Instance-ID is in the range from 0 to 64 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8, 9 to instance 10. By default, all VLANs are in instance 0. Use the no form of this command to remove VLAN from instance 1-64.

If you create 64 instances by stacking on a device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.

Configuration Examples

This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1.

```
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
-----------------------------------
Hostname(config-mst)# exit
Hostname(config)#
```

The following example removes VLAN3 from instance 1.

```
Hostname(config-mst)# no instance 1 vlan 3
```

The following example removes instance 1.

```
Hostname(config-mst)# no instance 1
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

6.7 l2protocol-tunnel stp

Use this command to enable BPDU TUNNEL globally. Use the **no** form of this command to disable this function.

l2protocol-tunnel stp

no l2protocol-tunnel stp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

Configuration Examples The following example enables BPDU TUNNEL globally.

```
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.8 l2protocol-tunnel stp enable

Use this command to enable BPDU TUNNEL on the interface. Use the **no** form of this command to disable this function.

l2protocol-tunnel stp enable

no l2protocol-tunnel stp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

Configuration Examples The following example enables BPDU TUNNEL on the interface.

```
Hostname(config-if-interface-id)# l2protocol-tunnel stp enable
Hostname(config-if-interface-id)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.9 l2protocol-tunnel stp tunnel-dmac

Use this command to configure the STP address for transparent transmission through BPDU TUNNEL. Use the **no** form of this command to restore the default setting.

l2protocol-tunnel stp tunnel-dmac *mac-address*

no l2protocol-tunnel stp tunnel-dmac

Parameter Description

Parameter	Description
mac-address	The STP address for transparent transmission.

Defaults The defualt is 01d0.f800.0005.

Command Mode Global configuration mode

Usage Guide The available STP address includes 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

Configuration Examples The following example configures the STP address for transparent transmission through BPDU TUNNEL.

```
Hostname(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.10 name

Use this command to set MST name. Use the **no** form of the command to restore the default setting.

name *name*

no name

Parameter Description

Parameter	Description
name	MST name, up to 32 characters.

Defaults The default is NULL.

Command Mode MST configuration mode

Usage Guide **name** *name*: Sets the MST name, up to 32 characters.

show spanning-tree mst configuration: Displays MST region information.

Configuration Examples This example sets MST name to region1.

```
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# name region1
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : ALL
Hostname(config-mst)# exit
```

```
Hostname(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.11 revision

Use this command to set revision number of MSTP region. Use the **no** form of the command to restore the default setting.

revision *version*

no revision

Parameter Description

Parameter	Description
version	MST revision number, in the range from 0 to 65535.

Defaults The default is 0.

Command Mode MST configuration mode

Usage Guide **revision** *version*: Sets the MST version, in the range from 0 to 65535.

show spanning-tree mst configuration: Displays MST region information.

Configuration Examples This example sets revision number to1.

```
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# revision 1
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name     :
Revision : 1
Instance  Vlans Mapped
--------  ----------------------------------------
0       : ALL
Hostname(config-mst)# exit
Hostname(config)#
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

6.12 spshow l2protocol-tunnel stp

Use this command to display BPDU TUNNEL configuration.

show l2protocol-tunnel stp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode / Global configuration mode / Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays BPDU TUNNEL configuration.

```
Hostname# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address:011a.a900.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.13 show spanning-tree

Use this command to display the global spanning-tree configuration.

show spanning-tree [summary | forward-time | hello-time | max-age | inconsistentports| tx-hold-count | pathcost method | max_hops | counters]

Parameter Description

Parameter	Description

summary	Displays the information of MSTP instances and forwarding status of the interfaces.
inconsistentports	Displays the block port due to root guard or loop guard.
forward-time	Displays BridgeForwardDelay.
hello-time	Displays BridgeHelloTime.
max-age	Displays BridgeMaxAge.
max-hops	Displays the maximum hops of an instance.
tx-hold-count	Displays TxHoldCount.
pathcost method	Displays the method used for calculating path cost.
counters	Displays the statistics of STP transceived packets.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the global spanning-tree configuration.

```
Hostname# show spanning-tree hello-time
```

The following example displays the sent and received STP packets.

```
Hostname# show spanning-tree counters
---------------------- STP BPDU count ----------------------
 Port                            Receive      Send
 GigabitEthernet 0/3             0            122594

------------------------- STP TC or TCN count -------------------------
 MSTID      Port                            Receive      Send
 0          GigabitEthernet 0/3             0            0
```

Related Commands

Command	Description
spanning-tree pathcost method	Sets the pathcost method.
spanning-tree forward-time	Sets BridgeForwardDelay.
spanning-tree hello-time	Sets BridgeHelloTime.
spanning-tree max-age	Sets BridgeMaxAge.
spanning-tree max-hops	Sets the maximum hops of an instance.
spanning-tree tx-hold-count	Displays TxHoldCount.

Platform Description N/A

6.14 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-id* [{ **bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter Description

Parameter	Description
interface-id	Interface ID
bpdufilter	Displays the status of BPDU filter.
portfast	Displays the status of portfast.
bpduguard	Displays the status of BPDU guard.
link-type	Displays the link type of an interface.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the STP configuration on interface Gi 0/1.

```
Hostname# show spanning-tree int gi 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
```

Related Commands

Command	Description
spanning-tree bpdufilter	Enables the BPDU filter feature someone the interface.
spanning-tree portfast	Enables the portfast on the interface.
spanning-tree bpduguard	Enables the BPDU guard on the interface.
spanning-tree link-type	Sets the link type of the interface to point-to-point.

Platform Description N/A

6.15 show spanning-tree mst

Use this command to display the information of MST and instances.

show spanning-tree mst { **configuration** | *instance-id* [**interface** *interface-id*] }

Parameter Description

Parameter	Description
configuration	The MST configuration of the equipment.
instance-id	Instance number
interface-id	Interface number

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information of MST and instances.

```
Hostname# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : test
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : 2-4094
1       : 1
```

Field Description

Field	Description
Multi spanning tree protocol	Enables MSTP protocol.
Name	Name of the MST region
Revision	Revision of the MST region
Instance Vlans Mapped	Mapping relation between the instance and VLAN

Related Commands

Command	Description
spanning-tree mst configuration	Configures the MST region.
spanning-tree mst cost	Displays the path cost of the instance.
spanning-tree mst max-hops	Displays the maximum hops of the instance.
spanning-tree mst priority	Displays the equipment priority of the instance.
spanning-tree mst port-priority	Displays the port priority of the instance.

Platform Description N/A

6.16 show spanning-tree mst topochange record

Use this command to display the STP topology change record.

show spanning-tree mst *instance-id* **topochange record**

Parameter Description

Parameter	Description
instance-id	Instance ID.

Defaults N/A

Command Mode Privileged EXEC mode / Global configuration mode / Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the STP topology change record of instance 0.

```
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   GI0/6              Learning     Forwarding   Normal
```

Field	Description

Time	The time when the topology changes.
Interface	The interface whose topology changes.
Old status	Old STP status on the interface.
New status	New STP status on the interface.
Type	Topology change may be caused by the following causes: Normal: UP/DOWN state change on the interface, LoopGuard Block: Loop-inconsistence causes the interface to be blocked. RootGuard Block: Root-inconsistence causes the interface to be blocked. Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked. LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence. Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.17 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

Parameter Description

Parameter	Description
forward-time *seconds*	Interval at which the port status changes, in the range from 4 to 30 in the unit of seconds. The default is 15.
hello-time *seconds*	Interval at which the switch sends the BPDU message, in the range

	from 1 to 10 in the unit of seconds. The default is 2.
max-age *seconds*	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The values of **forward-time, hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values.
2*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd)
If the values do not according with the condition, the settings do not work.

Configuration Examples The following example enables the spanning-tree function.

```
Hostname(config)# spanning-tree
```

The following example configures the BridgeForwardDelay.

```
Hostname(config)# spanning-tree  forward-time 10
```

Related Commands

Command	Description
show spanning-tree	Displays the global STP configuration.
spanning-tree mst cost	Sets the PathCost of an STP interface.
spanning-tree tx-hold-count	Sets the global TxHoldCount of STP.

Platform Description N/A

6.18 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** form of this command to disable this function.
spanning-tree autoedge [**disabled**]

Parameter Description

Parameter	Description
disabled	Disabled Autoedge on the interface.

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.
You can run the spanning-tree autoedge disabled command to disable Auto Edge.

Configuration Examples The following example disables Autoedge on the interface.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id-interface-id)# spanning-tree autoedge
disabled
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration information of the interface.

Platform Description N/A

6.19 spanning-tree bpdufilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.
spanning-tree bpdufilter [**enabled** | **disabled**]

Parameter Description

Parameter	Description
enabled	Enables BPDU filter on the interface.
disabled	Disables BPDU filter on the interface.

Defaults This function is disabled by default,

Command Mode Interface configuration mode.

Usage Guide If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Configuration Examples The following example enables BPDU filter on interface Gi 1/1.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id-interface-id)# spanning-tree bpdufilter
enable
```

Related

Command	Description

Commands		
	show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.20 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.

spanning-tree bpduguard [**enabled** | **disabled**]

Parameter Description

Parameter	Description
enabled	Enables BPDU guard on the interface.
disabled	Disables BPDU guard on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

1. If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
2. Run command **errdisable recovery** [**interval** *seconds*] to recover the interface in Error-disabled state.

Configuration Examples The following example enables the BPDU guard function on the interface.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id-interface-id)# spanning-tree bpduguard
enable
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.21 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attribute of current port to realize interconnection with other vendors. Use the **no** form of this

command to restore the default setting.

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default. .

Command Mode Interface configuration mode.

Usage Guide If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between our devices and other SPs' devices.

Configuration Examples The following example enables the compatibility mode on interface Gi 0/1.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-interface-id-interface-id)#spanning-tree compatible
enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.22 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide
1. Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.
2. The loop guard function and root guard function cannot be enabled at the same time.

Configuration Examples The following example enables **loop guard** on interface Gi 0/1.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-interface-id)# spanning-tree guard loop
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.23 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to enable this function

spanning-tree guard none

no spanning-tree guard none

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example disables **guard** on interface Gi 0/1.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-interface-id)# spanning-tree guard none
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.24 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to restore the default setting.

spanning-tree guard root

no spanning-tree guard root

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

3. If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.
4. The loop guard function and root guard function cannot be enabled at the same time.

Configuration Examples The following example enables **root guard** on the interface.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-interface-id)# spanning-tree guard root
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.25 spanning-tree ignore tc

Use this command to enable the tc filtering on the interface. Use the **no** form of this command to restore the default setting. With tc filtering enabled, the TC packets received on the interface will not be processed.

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide If TC filter is enabled on a port, the port does not process received TC packets.

Configuration Examples The following example enables the tc filtering on the interface.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-interface-id)# spanning-tree ignore tc
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.26 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of this command to restore the default setting.

spanning-tree link-type [**point-to-point** | **shared**]

no spanning-tree link-type

Parameter Description

Parameter	Description
point-to-point	Sets the link type of the interface to point-to-point.
shared	Forcibly sets the link type of the interface to shared.

Defaults For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.

Command Mode Interface configuration mode.

Usage Guide If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Configuration Examples The following example configures the link type of the interface.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id)# spanning-tree link-type point-to-point
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.27 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to restore the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Configuration Examples The following example enables **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu.

```
Hostname(config)# spanning-tree loopguard default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.28 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before being dropped. This parameter takes effect for all instances. Use the **no** form of this command to restore the default setting.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter Description

Parameter	Description
hop-count	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Defaults The default is 20 hops.

Command Mode Global configuration mode.

Usage Guide In the region, the BPDU message sent by the root bridge includes a Hot Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the max-hops command affects all instances.

Configuration Examples This example sets the max-hops of the spanning tree to 10 for all instances.

```
Hostname(config)# spanning-tree  max-hops 10
```

Related Commands

Command	Description
show spanning-tree	Displays the MSTP information.

Platform Description N/A

6.29 spanning-tree mode

Use this command to set the STP version. Use the **no** form of the command to restore the default setting.

spanning-tree mode [**stp** | **rstp** | **mstp**]

no spanning-tree mode

Parameter Description

Parameter	Description

stp	Spanning tree protocol(IEEE 802.1d)
rstp	Rapid spanning tree protocol(IEEE 802.1w)
mstp	Multiple spanning tree protocol(IEEE 802.1s)

Defaults The default is **mstp**.

Command Mode Global configuration mode.

Usage Guide However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with our devices, run this command to switch the STP mode to a lower version.

Configuration Examples The following example sets the STP version.

```
Hostname(config)# spanning-tree mode stp
```

Related Commands

Command	Description
show spanning-tree	Displays the spanning-tree configuration.

Platform Description N/A

6.30 spanning-tree mst configuration

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore the default setting.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode Global configuration mode.

Usage Guide To return to the privileged EXEC mode, enter end or Ctrl+C.

To return to the global configuration mode, enter exit.

After entering the MST configuration mode, you can configure MSTP Region parameters:

Configuration Examples This example enters the MST configuration mode.

```
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan  3, 5-10
Hostname(config-mst)# name region 1
Hostname(config-mst)# revision  1
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 1Instance  Vlans Mapped
----------  ---------------------
0       1-2,4,11-4094
1       3,5-10
-----------------------------------
Hostname(config-mst)# exit
Hostname(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MST region configuration.
instance *instance-id* **vlan** *vlan-range*	Adds VLANs to the MST instance.
name	Configures the name of MST.
revision	Configures the version of MST.

Platform Description N/A

6.31 anning-tree mst cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter Description

Parameter	Description
instance-id	Instance ID in the range from 0 to 64.
cost	Path cost in the range from 1 to 200,000,000.

Defaults The default instance-id is 0.

The default value is calculated by the link rate of the interface automatically.

1000 Mbps—20000
100 Mbps—200000
10 Mbps—2000000

Command Mode Interface configuration mode.

Usage Guide A higher cost value means a higher path cost.

Configuration Examples This example sets the path cost to 400 on the interface associated with instances 3.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# spanning-tree mst 3 cost 400
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst port-priority	Configures the priority of an interface.
spanning-tree mst priority	Configures the priority of an instance.

Platform Description N/A

6.32 spanning-tree mst port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of this command to restore the default setting.

spanning-tree [**mst** *instance-id*] **port-priority** *priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter Description

Parameter	Description
instance-id	Instance ID, in the range of 0 to 64
priority	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.

Defaults The default instance-id is 0.
The default priority is 128.

Command Mode Interface configuration mode.

Usage Guide When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.
Run this command to determine which port in the loop of a region enters the forwarding state.

Configuration Examples This example sets the priority of **gigabitethernet 1/1** to 10 in instance 20.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id)# spanning-tree mst 20 port-priority 0
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets the path cost.
spanning-tree mst priority	Sets the device priority for different instances.

Platform Description N/A

6.33 spanning-tree mst priority

Use this command to set the device priority for different instances in the global configuration mode.
Use the **no** form of this command to restore the default setting.
spanning-tree [**mst** *instance-id*] **priority** *priority*
no spanning-tree [**mst** *instance-id*] **priority**

Parameter Description

Parameter	Description
instance-id	Instance ID, in the range of 0 to 64
priority	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440, which are all multiples of 4096.

Defaults The default instance ID is 0.
The default device priority is 32768.

Command Mode Global configuration mode.

Usage Guide Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuration Examples The following example sets the device priority of the Instance to 8192.

```
Hostname(config)# spanning-tree mst 20 priority 8192
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets path cost.
spanning-tree mst port-priority	Sets the port priority of an instance.

Platform Description N/A

6.34 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of this command to restore the default setting.

spanning-tree pathcost method { { **long** [**standard** } | **short** }

no spanning-tree pathcost method

Parameter Description

Parameter	Description
Long [**standard**]	Adopts the 802.1t standard to configure path cost. The standard indicates that use the expression recommended by the standard to calculate the cost value.
short	Adopts the 802.1d standard to configure path cost.

Defaults 802.1T standard is adopted to set path cost by default.

Command Mode Global configuration mode.

Usage Guide If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Configuration Examples The following example configures the path cost of the port.

```
Hostname(config-if)# spanning-tree pathcost method long
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.35 spanning-tree portfast

Use this command to enable the portfast on the interface. Use the disabled form of this command to restore the default setting,

spanning-tree portfast [**disabled**]

Parameter Description

Parameter	Description
disabled	Disables the portfast on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

Configuration Examples The following example enables the portfast on the interface.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if-interface-id)# spanning-tree portfast
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.36 spanning-tree portfast bpdufilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to restore the default setting.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default,

Command Mode Global configuration mode.

Usage Guide Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the Port Fast interface. Use the **show spanning-tree** command to display the configuration.

Configuration Examples The following example enables the BPDU filter function globally.

```
Hostname(config)# spanning-tree portfast bpdufilter default
```

Related Commands

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

6.37 spanning-tree portfast bpduguard default

Use this command to enable the BPDU guard globally. Use the **no** form of this command to restore the default setting,

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.

The global BPDU guard takes effect only when PortFast is enabled on a port.

Configuration Examples The following example enables the GPDU guard globally.

```
Hostname(config)# spanning-tree portfast bpduguard
default
```

Related Commands

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

6.38 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of this command to restore the default setting.

spanning-tree portfast default

no spanning-tree portfast default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the portfast feature on all interfaces globally.

```
Hostname(config)# spanning-tree portfast default
```

Related Commands

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

6.39 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default setting.

spanning-tree reset

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode.

Usage Guide The function do not have a **no** command.

Configuration Examples The following example resets STP.

```
Hostname(config)# spanning-tree reset
```

Related Commands

Command	Description
show spanning-tree	Displays the global STP configuration.
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

6.40 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable this function on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading

Configuration Examples The following example enables **tc-guard** on the interface to prevent the spread of TC messages.

```
Hostname(config)# spanning-tree tc-guard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.41 spanning-tree tc-protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable this function.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables **tc-protection** globally.

```
Hostname(config)# spanning-tree tc-protection
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.42 spanning-tree tc-protection tc-guard

Use this command to enable tc-guard to prevent TC packets from being flooded. Use the **no** form of this command to restore the default setting.

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading.

Configuration Examples The following example enables tc-guard to prevent TC packets from being flooded.

```
Hostname(config)# spanning-tree tc-protection tc-guard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.43 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP, the maximum number of the BPDU messages sent in one second. Use the **no** form of this command to restore the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter Description

Parameter	Description
*tx-hold-coun*t	Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the BPDU messages sent in one second.

```
Hostname(config)# spanning-tree tx-hold-count 5
```

Related Commands

Command	Description
show spanning-tree	Displays the global MSTP configuration.

Platform Description N/A

7 LLDP Commands

7.1 { voice | voice-signaling } vlan

Use this command to configure the LLDP network policy. Use the **no** form of this command to delete the policy.

{ **voice | voice-signaling** } **vlan** { { *vlan-id* [**cos** *cvalue* **| dscp** *dvalue*] } | { **dot1p** [**cos** *cvalue* **| dscp** *dvalue*] } **| none | untagged** }

no { **voice | voice-signaling** } **vlan**

Parameter Description

Parameter	Description
voice	Voice application
voice-signaling	Voice-signaling application
vlan-id	(Optional) VLAN ID of voice flow. The value ranges from 1 to 4094.
cos	(Optional) Class of service
cvalue	(Optional) CoS of the configured voice flow. The value ranges from 0 to 7, and the default value is **5**.
dscp	(Optional) Differentiated services code point
dvalue	(Optional) DSCP value of the configured voice flow. The value ranges from 0 to 63. The default value is 46.
dot1p	(Optional) 802.1p priority tagging. The tag frame includes user_priority and vlan id is 0.
none	(Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration.
untagged	(Optional) The untag frame is sent in the voice vlan in VoIP. In this case, the value of vlan id and cos are ignored.

Defaults N/A

Command Mode LLDP network policy configuration mode

Usage Guide In the LLDP network policy configuration mode, configure the LLDP network policy.

Voice indicates the voice data type, and voice-signaling indicates the voice signal type.

If a device connects to an IP phone and the IP phone supports LLDP-MED, the network policy TLV can be configured to deliver policies to the IP phone, so that the IP phone changes the voice stream tag and QoS. Excluding the preceding policy, the following operations need to be performed on the device:

1. Enable the voice VLAN function and add the port connected to the IP phone to the voice VLAN in static mode.
2. Configure the port connected to the IP phone to a QoS trusted port. (It is recommended to use the

trusted DSCP mode.)
3. If 802.1X authentication is enabled on the port at the same time, a security channel needs to be configured to transmit packets from the voice VLAN.
If the IP phone does not support LLDP-MED, the voice VLAN function must be enabled. In addition, the MAC address of the IP phone needs to be added to the voice VLAN OUI list manually.

For details about how to configure the QoS trusted mode, see chapter "IP QoS." For details about how to configure the voice VLAN, see chapter "Voice VLAN." For details about how to configure the security channel, see chapter "ACL".

Configuration Examples The following example configures the LLDP network policy (profile-num is 1).

```
Hostname#config
Hostname(config)#lldp network-policy profile 1
Hostname(config-lldp-network-policy)# voice vlan untagged
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6
```

Related Commands

Command	Description
show lldp network-policy profile [*profile-num*]	Displays the LLDP network policy.

Platform Description N/A

7.2 civic-location

Use this command to configure a common LLDP address. Use the **no** form of this command to delete the address.

civic-location { **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 civic-location { **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*

Parameter Description

Parameter	Description
country	Country code, two bytes. For example, the country code of China is CH.
state	Address information, CA type 1
county	CA type 2

city	CA type 3
division	CA type 4
neighborhood	CA type 5
street-group	CA type 6
leading-street-dir	CA type 16
trailing-street-suffix	CA type 17
street-suffix	CA type 18
number	CA type 19
street-number-suffix	CA type 20
landmark	CA type 21
additional-location-information	CA type 22
name	CA type 23
postal-code	CA type 24
building	CA type 25
unit	CA type 26
floor	CA type 27
room	CA type 28
type-of-place	CA type 29
postal-community-name	CA type 30
post-office-box	CA type 31
additional-code	CA type 32
ca-word	Address information

Defaults N/A

Command Mode LLDP Civic address configuration mode

Usage Guide This command is used to configure a common LLDP address in LLDP Civic address configuration mode.

Configuration Examples The following example configures an LLDP Civic Address (ID: 1).

```
Hostname#config
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# country CH
Hostname(config-lldp-civic)# city Fuzhou
```

Related Commands

Command	Description
show lldp location civic-location { **identifier** *id* **| interface** *interface-name* **| static** }	Displays the information about an LLDP Civic address.

Platform Description N/A

7.3 clear lldp statistics

Use this command to clear LLDP statistics.

clear lldp statistics [**interface** *interface-name*]

Parameter Description	**Parameter**	**Description**
	interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide **interface** parameter: clear the LLDP statistics of the specified interface

Configuration Examples The following example clears LLDP statistics of interface 1.

```
Hostname# clear lldp statistics interface GigabitEthernet 0/1
Hostname# show lldp statistics interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 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
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

7.4 clear lldp table

Use this command to clear LLDP neighbor information.

clear lldp table [**interface** *interface-name*]

Parameter Description	**Parameter**	**Description**
	interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the **interface** parameter is specified, the LLDP neighbor information on the specified interface is cleared.
If the **interface** parameter is not specified, the LLDP neighbor information on all interfaces is cleared.

Configuration Examples The following example clears the LLDP neighbor information on interface 1.

```
Hostname# show lldp neighbors interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 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
Hostname# clear lldp table interface GigabitEthernet 0/1
Hostname# show lldp neighbors interface GigabitEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.5 device-type

Use this command to configure the device type. Use the **no** form of this command to restore the default setting.
device-type *device-type*
no device-type

Parameter Description

Parameter	Description
device-type	Device type. The value ranges from 0 to 2. 0: The device type is DHCP Server. 1: The device type is switch. 2: The device type is LLDP MED terminal.

Defaults

Command LLDP Civic address configuration mode

Mode

Usage Guide This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.

Configuration Examples The following example sets the device type to switch.

```
Hostname#config
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# device-type 1
```

Related Commands

Command	Description
show lldp location civic-location { **identifier** *id* **| interface** *interface-name* **| static** }	Displays LLDP Civic Address information.

Platform Description N/A

7.6 lldp compliance vendor

Use this command to enable detection of compatible neighbors.

lldp compliance vendor

no lldp compliance vendor

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables detection of compatible neighbors.

```
Hostname#configure terminal
Hostname(config)# lldp compliance vendor
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.7 lldp enable

Use this command to enable the LLDP globally or on the interface. Use **no** form of this command to disable this function.

lldp enable

no lldp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global (or interface) configuration mode

Usage Guide LLDP takes effect on an interface only when LLDP is enabled globally.

Configuration Examples The following example disables LLDP globally and on the interface.

```
Hostname#config
Hostname(config)#no lldp enable
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)# no lldp enable
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

7.8 lldp encapsulation snap

Use this command to configure the encapsulation format of LLDP packets. Use the **no** form of this command to restore the default setting.

lldp encapsulation snap

no lldp encapsulation snap

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, Ethernet II encapsulation format is used.

Command Interface configuration mode.

Mode

Usage Guide

To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.

Configuration Examples

```
The following example sets LLDP packet encapsulation format to
SNAP.Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp encapsulation snap
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description

N/A

7.9 lldp error-detect

Use this command to configure the LLDP error detection, including the detection of VLAN configurations on both sides of the link, port state detection, port aggregation configuration detection, MTU configuration detection and loop detection. If any error is detected by LLDP, warning message will be printed to notify the administrator. Use the **no** form of this command to disable this function.

lldp error-detect

no lldp error-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode.

Usage Guide

LLDP error detection relies on the specific TLV in the LLDP packets exchanged between devices on both sides of the link. To ensure normal functioning of the detection feature, correct TLVs must be advertised.

Configuration Examples

The following example configures LLDP error detection.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp error-detect
```

Related

Command	Description

Commands	show interface status	Displays LLDP status information.

Platform Description N/A

7.10 lldp fast-count

When a new neighbor is detected or when LLDP operating mode changes from shutdown or Rx to TxRx or Tx, to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism shortens the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs before restoring to the normal transmit interval. Use the **no** form of this command to restore the default setting.

lldp fast-count *value*

no lldp fast-count

Parameter Description

Parameter	Description
value	The number of fast sent LLDP packets, in the range from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the number of fast sent LLDP packets to 5.

```
Hostname#config
Hostname(config)#lldp fast-count 5
```

Related Commands

Command	Description
show interface status	Displays LLDP status information.

Platform Description N/A

7.11 lldp hold-multiplier

Use this command to set the TTL multiplier. Use the **no** form of this command to restore to default setting.

lldp hold-multiplier *value*

no lldp hold-multiplier

Parameter

Parameter	Description

Description	*value*	TTL multiplier, in the range from 2 to 10.

Defaults The default is 4.

Command Mode Global configuration mode.

Usage Guide The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

Configuration Examples The following example sets TTL multiplier to 5.

```
Hostname#config
Hostname(config)#lldp hold-multiplier 5
```

Related Commands	**Command**	**Description**
	show lldp status	Displays LLDP status information.

Platform Description N/A

7.12 lldp location civic-location identifier

Use this command to create a common address of a device connected to the network in LLDP Civic Address configuration mode. Use the **no** form of this command to delete the address.

lldp location civic-location identifier *id*

no lldp location civic-location identifier *id*

Parameter Description	**Parameter**	**Description**
	id	ID of a common address of a network device, in the range from 1 to 1024.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command can be used to enter the LLDP Civic Address configuration mode.

Configuration Examples The following example creates the Civic Address information in LLDP MED-TLV as follows: set *id* to **1**.

```
Hostname#config
Hostname(config)#lldp location civic-location identifier 1
```

```
Hostname(config-lldp-civic)#
```

Related Commands	Command	Description
	show lldp location civic-location { **identifier** *id* **| interface** *interface-name* **| static** }	Displays the LLDP Civic Address information.

Platform Description N/A

7.13 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the **no** form of this command to delete the number.

lldp location elin identifier *id* **elin-location** *tel-number*

no lldp location elin identifier *id*

Parameter Description	Parameter	Description
	id	ID of an emergency number, in the range from 1 to 1024.
	tel-number	Emergency number, in the range from 10 to 25 bytes.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure an emergency number.

Configuration Examples The following example sets an emergency number.

```
Hostname#config
Hostname(config)#lldp location elin identifier 1 elin-location 085283671111
```

Related Commands	Command	Description
	show lldp location elin-location { **identifier** *id* **| interface** *interface-name* **| static }**	Displays an LLDP emergency number.

Platform Description N/A

7.14 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Use the **no** form of this command to disable the advertisement of management address.

lldp management-address-tlv [*ip-address*]

no lldp management-address-tlv

Parameter Description	Parameter	Description
	ip-address	The management address advertised in LLDP packets.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide By default, the management address is advertised in LLDP packets, and is the IPv4 address of the lowest-ID VLAN carried on the port. If IPv4 address is not configured for this VLAN, the next lowest-ID VLAN carried on the port will be tried until the IPv4 address is obtained.
If the IPv4 address is still not found, the IPv6 address of the lowest-ID VLAN carried on the port will be tried.
If the IPv6 address is still not found, the MAC address of the device will be advertised as the management address.

Configuration Examples The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp management-address-tlv 192.168.1.1
```

Related Commands	Command	Description
	show lldp local-information	Displays LLDP local information

Platform Description N/A

7.15 lldp mode

Use this command to configure the LLDP operating mode. Use **no** form of this command to restore the default setting.
lldp mode { **rx** | **tx** | **txrx** }
no lldp mode

Parameter Description	Parameter	Description
	rx	Only sends LLDPDUs.
	tx	Only receives LLDPDUs.
	txrx	Sends and receives LLDPDUs.

Defaults The default is **txrx**.

Command Mode Interface configuration mode

Usage Guide Disable LLDP operating mode on the interface. The interface won't send and receive LLDP packets. The precondition for enabling LLDP on the interface is that LLDP has been enabled globally and LLDP operates in tx, rx or txrx mode.

Configuration Examples The following example sets LLDP operating mode to tx on the interface.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp mode tx
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information

Platform Description N/A

7.16 lldp network-policy profile

Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the no form of this command to delete the policy.

lldp network-policy profile *profile-num*

no lldp network-policy profile *profile-num*

Parameter Description

Parameter	Description
profile-num	ID of an LLDP network policy, in the range from 1 to 1024.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to enter the LLDP network policy configuration mode. When this command is run, the policy ID must be specified.

In LLDP network-policy mode, the { **voice** | **voice-signaling** } **vlan** command can be used to configure the specific network policy.

Configuration Examples The following example creates an LLDP network policy whose ID is 1.

```
Hostname#config
Hostname(config)#lldp network-policy profile 1
```

```
Hostname(config-lldp-network-policy)#
```

Related Commands	Command	Description
	show lldp network-policy profile [*profile-num*]	Displays an LLDP network policy.

Platform Description N/A

7.17 lldp notification remote-change enable

Use this command to configure LLDP Trap. Use the **no** form of this command to restore the default setting.

lldp notification remote-change enable

no lldp notification remote-change enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide By configuring LLDP Trap, the LLDP information of local device (such as information about the detection of new neighbor or the fault on the communication link) can be sent to the network management server. The administrator can monitor the network operation status according to such information.

Configuration Examples The following example configures LLDP Trap.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp notification remote-change enable
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

7.18 lldp timer notification-interval

Use this command to set an interval of sending LLDP Traps. Use the **no** form of this command to

restore the default setting.

lldp timer notification-interval *seconds*

no lldp timer notification-interval

Parameter Description	Parameter	Description
	seconds	Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds.

Defaults The default is 5.

Command Mode Global configuration mode.

Usage Guide To prevent excessive LLDP traps from being sent, you can set an interval of sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.

Configuration Examples The following example sets the interval of sending LLDP Traps to 10 seconds.

```
Hostname#config
Hostname(config)#lldp timer notification-interval 10
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

7.19 lldp timer reinit-delay

Use this command to set port initialization delay. Use the **no** form of this command to restore he default setting.

lldp timer reinit-delay *seconds*

no lldp timer reinit-delay

Parameter Description	Parameter	Description
	seconds	Port initialization delay, in the range from 1 to 10 in the unit of seconds.

Defaults The default is 2.

Command Mode Global configuration mode.

Usage Guide To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

Configuration Examples The following example sets LLDP port initialization delay to 3 seconds.

```
Hostname#config
Hostname(config)#lldp timer reinit-delay 3
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

7.20 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Use the **no** form of this command to restore the default setting.

lldp timer tx-delay *seconds*

no lldp timer tx-delay

Parameter Description

Parameter	Description
seconds	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.

Defaults The default is 2.

Command Mode Global configuration mode.

Usage Guide An LLDP-enabled port will send LLDP packets when the local device information changes. To avoid frequently sending LLDP packets due to the frequent local device information change, configure the LLDP packet transmission delay to control the frequent transmission of LLDP packets.

Configuration Examples The following example sets LLDPDU transmission delay to 3 seconds.

```
Hostname#config
Hostname(config)#lldp timer tx-delay 3
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

7.21 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Use **no** form of this command to restore the default setting.

lldp timer tx-interval *seconds*

no lldp timer tx-interval

Parameter Description

Parameter	Description
seconds	Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds.

Defaults The default is 30.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the interval of sending the LLDP packets to 10 seconds.

```
Hostname#config
Hostname(config)#lldp timer tx-interval 10
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

7.22 lldp tlv-enable

Use this command to configure the types of advertisable TLVs. Use the **no** form of this command to restore the default setting.

lldp tlv-enable { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id** [*vlan-id*] **| vlan-name** [*vlan-id*] } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv** { **all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }

no lldp tlv-enable { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv** { **all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }

Parameter Description

Parameter	Description
basic-tlv	Basic management TLV
port-description	Port Description TLV
system-capability	System Capabilities TLV
system-description	System Description TLV
system-name	System Name TLV
dot1-tlv	802.1 organizationally specific TLV
port-vlan-id	Port VLAN ID TLV
protocol-vlan-id	Port And Protocol VLAN ID TLV
vlan-id	VLAN ID
vlan-name	VLAN Name TLV
vlan-id	VLAN ID corresponding to the specified VLAN name
dot3-tlv	802.3 organizationally specific TLV
link-aggregation	Link Aggregation TLV
mac-physic	MAC/PHY Configuration/Status TLV
max-frame-size	Maximum Frame Size TLV
power	Power Via MDI TLV
med-tlv	LLDP MED TLV
capability	LLDP-MED Capabilities TLV
inventory	Inventory management TLVs, including hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.
location	Location Identification TLV
civic-location	Common address information about the network device in location identification TLVs.
elin	Encapsulated emergency number
id	Policy ID
network-policy	Network Policy TLV
profile-num	ID of network policy
power-over-ethernet	Extended Power-via-MDI TLV

Defaults By default, all TLVs other than Location Identification TLV can be advertised on the interface for products other than S12000. For the S12000 product series, only basic TLVs and IEEE 802.1 TLVs are advertised. To advertise IEEE 802.3 TLVs and LLDP-MED TLVs, run the **lldp tlv-enable** command.

Command Interface configuration mode

Mode

Usage Guide During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the **all** parameter is specified, all optional TLVs of the types are advertised.
During configuration of LLDP-MED TLVs, if the **all** parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised.
When configuring LLDP-MED Capability TLVs, configure LLDP-MED MAC/PHY TLVs first. When canceling LLDP-MED MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first.
When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured.
To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED Capability TLVs can be canceled.

Configuration Examples The following example configures all IEEE 802.1 TLVs to be advertised.

```
Hostname# configure terminal
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
```

The following example applies LLDP network policy 1 on the 0/1 interface.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv
network-policy profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location
civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/1 interface.

```
Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp location elin identifier 1
```

Related Commands

Command	Description
show lldp tlv-config interface	Displays the attributes of advertisable TLVs

Platform Description N/A

7.23 show lldp local-information

Use this command to display the LLDP information of local device. The information will be

encapsulated in the TLVs and sent to the neighbor device.

show lldp local-information [**global** | **interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

- **global** parameter: display the global LLDP information to be sent.
- **Interface** parameter: displays the LLDP information to be sent out the interface specified.
- No parameter: display all LLDP information, including global and interface-based LLDP information.

Configuration Examples The following example displays the device information to be sent to neighbor device.

```
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     :S2915-L_RGOS 11.4(1)B82, Release(09230219)
 SerialNum      : 1234942570001
 Manufacturer name    : Manufacturer name
 Asset tracking identifier   :
----------------------------------------------------------
Lldp local-information of port [GigabitEthernet 0/1]
----------------------------------------------------------
 Port ID type     : Interface name
 Port id      : GigabitEthernet 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 : 100BASE-TX full duplex mode, 100BASE-TX half
duplex mode
Operational MAU type    :
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
```

show lldp local-information command output description:

Field	Description
Chassis ID type	Chassis ID type for identifying the Chassis ID field
Chassis ID	Used to identify the device, and is generally represented with MAC address
System name	Name of the sending device
System description	Description of the sending device, including hardware/software version, operating system and etc.

System capabilities supported	Capabilities supported by the system
System capabilities enabled	Capabilities currently enabled by the system
LLDP-MED capabilities	LLDP-MED capabilities supported by the system
Device class	MED device class, which is divided into 2 categories: network connectivity device and terminal device. Network connectivity device Class I: normal terminal device Class II: media terminal device; besides Class I capabilities, it also supports media streams. Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication.
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Device manufacturer
Asset tracking identifier	Asset tracking ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Management address subtype	Management address type
Management address	Management address
Interface numbering subtype	Type of the interface identified by the management address
Interface number	ID of the interface identified by the management address
Object identifier	ID of the object identified by the management address
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID	Port and Protocol VLAN ID
PPVID Supported	Indicates whether port and protocol VLAN is supported
PPVID Enabled	Indicates whether port and protocol VLAN is enabled
VLAN name of VLAN 1	Name of VLAN 1
Protocol Identity	Protocol identifier
Auto-negotiation supported	Indicates whether auto-negotiation is supported
Auto-negotiation enabled	Indicates whether auto-negotiation is enabled
PMD auto-negotiation advertised	Auto-negotiation advertising capability of the port
Operational MAU type	Speed and duplex state of the port
PoE support	Indicates whether POE is supported
Link aggregation supported	Indicates whether link aggregation is supported
Link aggregation enabled	Indicates whether link aggregation is enabled
Aggregation port ID	ID of the link aggregation port
Maximum frame Size	Maximum frame size supported by the port

Power-via-MDI device type	Device type, including: PSE (power sourcing equipment) PD (powered device)
Power-via-MDI power source	Power source type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Available power on port
Model name	Name of model

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.24 show lldp location

Use this command to display the common LLDP address or emergency number of the local device.

show lldp location { **civic-location | elin** } { **identifier** *id* **| interface** *interface-name* **| static** }

Parameter Description

Parameter	Description
civic-location	Encapsulates a common address of a network device.
elin	Encapsulates an emergency number.
identifier	Displays one address or emergency number configured.
id	Policy ID of configured information
interface	Displays the address or emergency number on an interface.
interface-name	Interface name
static	Displays all addresses or emergency numbers configured.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the policy ID is specified, the specified address or emergency number is displayed.
If the interface name is specified, the address or emergency number configured on the interface is displayed.
If no parameter is specified, all addresses or emergency numbers are displayed.

Configuration Examples The following example displays all addresses.

```
Hostname# show lldp location civic-location static
LLDP Civic location information
-------------------------
```

```
Identifier    : testt
County     : china
City Division    : 22
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     : Gi0/1
--------------------------
Identifier    : tee
--------------------------
```

The following example displays all emergency numbers.

```
Hostname# show lldp location elin-location static
Elin location information
--------------------------
Identifier : t
Elin  : iiiiiiiiii
Ports     : Gi1/0/3
--------------------------
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.25 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

show lldp neighbors [**interface** *interface-name*] [**detail**]

Parameter Description	Parameter	Description
	interface-name	Interface name
	detail	All information about a neighboring device

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the **detail** parameter is not specified, the brief information about a neighboring device is displayed. If the **detail** parameter is specified, the detailed information about a neighboring device is displayed. If the **interface** parameter is specified, the neighboring device information received on the specified interface is displayed.

Configuration Examples The following example displays the neighboring device information received on all ports.

```
Hostname# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 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      : GigabitEthernet 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   :
```

Description of fields:

Field	Description
Neighbor index	Neighbor index
Device type	Type of neighboring device
Update time	Latest update time of neighbor information
Aging time	Aging time of a neighbor, namely the time after which a neighbor is aged and deleted
Chassis ID type	Chassis ID type
Chassis ID	Used to identify a device. Usually, a MAC address is used.
System name	Device name
System description	Device description, including hardware/software version and operating system
System capabilities supported	Functions supported by the system
System capabilities enabled	Functions enabled by the system
Management address subtype	Type of management address
Management address	Management address
Interface numbering subtype	Interface type of management address
Interface number	Interface ID of management address

Object identifier	Object ID of management address
Device class	MED device type: network connectivity device and terminal device Network connectivity device: Class I: general terminal device Class II: media terminal device, including capabilities of Class I and supporting media stream Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name
Asset tracking identifier	Asset ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Port VLAN ID	VLAN ID of a port
Port and protocol VLAN ID	Port and protocol VLAN ID
PPVID Supported	Whether port and protocol VLAN is supported
PPVID Enabled	Whether port and protocol VLAN is enabled
VLAN name of VLAN 1	VLAN 1 name
Protocol Identity	Protocol ID
Auto-negotiation supported	Whether auto-negotiation is supported
Auto-negotiation enabled	Whether auto-negotiation is enabled
PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
Operational MAU type	Rate and duplex status of port auto-negotiation
PoE support	Whether POE is supported
Link aggregation supported	Whether link aggregation is supported
Link aggregation enabled	Whether link aggregation is enabled
Aggregation port ID	ID of link aggregation port
Maximum frame Size	Maximum frame length supported by a port
Power-via-MDI device type	Device type, including: ● PSE ● PD
Power-via-MDI power source	Power type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Power value of a port where power is supplied

Related	**Command**	**Description**

Commands	N/A	N/A

Platform Description N/A

7.26 show lldp network-policy profile

Use this command to display the information about an LLDP network policy.

show lldp network-policy { **profile** [*profile-num*] | **interface** *interface-name* }

Parameter Description

Parameter	Description
profile-num	ID of a network policy, in the range from 1 to 1024.
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If *profile-num* is specified, the information about the specified network policy is displayed.
If no parameter is specified, the information about all network policies is displayed.

Configuration Examples

```
The following example displays the information about a network policy.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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.27 show lldp statistics

The following example displays LLDP statistics.

show lldp statistics [**global** | **interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

- **global** parameter: display the global LLDP statistics.
- **Interface** parameter: display the LLDP statistics of the specified interface.

Configuration Examples The following example displays all LLDP statistics.

```
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 [GigabitEthernet 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
```

show lldp statistics command output description:

Field	Description
Neighbor information last change time	Time the neighbor information is latest updated
The number of neighbor information inserted	Number of times of adding neighbor information
The number of neighbor information deleted	Number of times of removing neighbor information
The number of neighbor information dropped	Number of times of dropping neighbor information
The number of neighbor information aged out	Number of the neighbor information entries that have aged out
The number of lldp frames transmitted	Total number of the LLDPDUs transmitted

The number of frames discarded	Total number of the LLDPDUs discarded
The number of error frames	Total number of the LLDP error frames received
The number of lldp frames received	Total number of the LLDPDUs received
The number of TLVs discarded	Total number of the LLDP TLVs dropped
The number of TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized
The number of neighbor information aged out	Number of the neighbor information entries that have aged out

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.28 show lldp status

Use this command to display LLDP status information.

show lldp status [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide **interface** parameter: display the LLDP status information of the specified interface.

Configuration Examples The following example displays LLDP status information of all ports.

```
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 [GigabitEthernet 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
```

show lldp status command output description:

Field	Description
Global status of LLDP	Whether LLDP is globally enabled
Neighbor information last changed time	Time the neighbor information is latest updated
Transmit interval	LLDPDU transmit interval
Hold multiplier	TTL multiplier
Reinit delay	Port re-initialization delay
Transmit delay	LLDPDU transmit delay
Notification interval	Interval for sending LLDP Traps
Fast start counts	The number of fast sent LLDPDUs
Port status of LLDP	Whether LLDP is enabled on the port
Port state	Link status of port: UP or DOWN
Port encapsulation	LLDPDU encapsulation format
Operational mode	Operating mode of LLDP
Notification enable	Whether LLDP Trap is enabled on the port
Error detect enable	Whether error detection is enabled on the port
Number of neighbors	Number of neighbors
Number of MED neighbors	Number of MED neighbors

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.29 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

show lldp tlv-config [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide **Interface** parameter: display the LLDP TLV configuration of the specified interface.

Configuration Examples The following example displays TLV information of port 1.

```
Hostname# show lldp tlv-config interface GigabitEthernet 0/1
LLDP tlv-config of port [GigabitEthernet 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8 QinQ Commands

8.1 dot1q new-outer-vlan *new-vid* translate old-outer-vlan *vid* inner-vlan *v-list*

Use this command to modify the policy list of outer vid based on the inner Tag VID and outer Tag VID on the access, trunk, hybrid, uplink port. Use the **no** form of this command to restore the default setting.

dot1q new-outer-vlan *new-vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

no dot1q new-outer-vlan *new-vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

Parameter Description

Parameter	Description
new-vid	Vid list of the
vid	Vid of outer tag.
no	Removes the setting.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A.

Configuration Examples The following example modifies the vid to 3888 when the input packets inner tag vid.

```
Hostname(config)# vlan 1888, 3888
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# dot1q new-outer-vlan 3888 translate old-outer-vlan 1888
inner-vlan 2001-3000
Hostname(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.2 dot1q outer-vid vid register inner-vid v-list

Use this command to configure the add policy list of outer vid based on protocol on tunnel port. Use the **no** or **default** form of this command to restore the default setting.

dot1q outer-vid *vid* **register inner-vid** *v_list*

no dot1q outer-vid *vid* **register inner-vid** *v_list*

Parameter Description

Parameter	Description
v_list	Inner vlan id list
vid	Outer vlan id list

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies vid in the tag of input message as 4-22 and setss the vid to 3.

```
Hostname#configure
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if)#switchport mode dot1q-tunnel
Hostname(config-if)#dot1q outer-vid 3 register inner-vid 4-22
Hostname(config-if)#end
```

Related Commands

Command	Description
show registration-table [**interface** *intf-id*]	N/A

Platform Description N/A

8.3 dot1q relay-vid vid translate local-vid v-list

Use this command to configure the modify policy list of outer vid based on protocol on access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

dot1q relay-vid *vid* **translate local-vid** *v-list*

no dot1q relay-vid *vid* **translate local-vid** *v-list*

default dot1q relay-vid *vid* **translate local-vid** *v-list*

Parameter Description

Parameter	Description

v_list	Outer vlan list of input message
vid	Modified outer vlan id list
no	Removes the settings.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies vid in the outer tag of input message as 10-20 and sets the vid to 100.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if)# switchport mode access
Hostname(config-if)# dot1q relay-vid 100 translate local-vid 10-20
Hostname(config-if)# end
```

Related Commands

Command	Description
show translation-table [interface *intf-id*]	N/A

Platform Description N/A

8.4 dot1q relay-vid vid translate inner-vid v-list

Use this command to configure the modify policy list of outer vid based on protocol on access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

dot1q relay-vid *vid* **translate inner-vid** *v-list*

no dot1q relay-vid *vid* **translate inner-vid** *v-list*

default dot1q relay-vid *vid* **translate inner-vid** *v-list*

Parameter Description

Parameter	Description
v_list	Outer vlan list of input message
vid	Modified outer vlan id list

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures vid in the outer tag of input message as 10-20 and sets the vid to 100.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if)# switchport mode access
Hostname(config-if)# dot1q relay-vid 100 translate inner-vid 10-20
Hostname(config-if)# end
```

Related Commands

Command	Description
show translation-table [interface *intf-id*]	N/A

Platform Description N/A

8.5 dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

Use this command to map the priority from the outer tag to the inner tag for the packets on the interface. Use the **no** form of this command to restore the default setting.

dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

no dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

default dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

Parameter Description

Parameter	Description
inner-cos-value	Indicates the CoS value of the inner tag.
outer-cos-value	Indicates the CoS value of the outer tag.
no	Cancels the priority mapping of the packets on the interface.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide If the QoS policy based on the COS value is set for the service provider's network to which a user network connects, the COS value of the outer tag can be set to different values based on the data packet importance. In this case, important services can be preferentially processed and transmitted.

Configuration Examples The following example configures the priority mapping from the outer tag to the inner tag.

```
Hostname# configure
Hostname(config)# interface gigabitEthernet 0/2
Hostname(config-if)# dot1q-tunnel cos 3 remark-cos 5
Hostname(config-if)# end
```

Related Commands

Command	Description
show interface intf-name remark	N/A

Platform Description N/A

8.6 frame-tag tpid

Use this command to set the packet TPID compatible with the manufacturer TPID. Use the **no** or **default** form of this command to restore the default setting.

frame-tag tpid *tpid*

no frame-tag tpid

default frame-tag tpid

Parameter Description

Parameter	Description
tpid	Packet TPID.

Defaults The default is 0x8100.

Command Mode Interface configuration mode.

Usage Guide If the TPID value of the connected third-party device is not 0x8100 (default value) defined in IEEE802.1Q, the TPID value on the egress used to connect to the third-party device is the TPID value of the third-party device.

Configuration Examples The following example sets the packet TPID compatible with the manufacturer TPID.

```
Hostname(config)# interface g0/3
Hostname(config-if)# frame-tag tpid 0x9100
Hostname(config-if)# end
Hostname# show frame-tag tpid
Port    tpid
------  ---------
Gi0/3    0x9100
```

Related Commands

Command	Description
show frame-tag tpid	N/A

Platform N/A

Description

8.7 inner-priority-trust enable

Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface. Use the **no** or **default** form of this command to restore the default setting.

inner-priority-trust enable

no inner-priority-trust enable

default inner-priority-trust enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide If the QoS policy is configured based on the COS value of the user's VLAN tag for the service provider's network to which a user network connects, the user's VLAN tag priority can be copied to the outer VLAN tag, so that the user's packets are encapsulated with the outer VLAN tag and have the same priority as the user's VLAN tag. In this case, the user's packets can be preferentially processed and transmitted on the service provider's network.

Configuration Examples The following example copies the priority of the inner tag to the outer tag of the packets on the interface.

```
Hostname#configure terminal
Hostname(config)# interface gigabitEthernet 0/2
Hostname(config-if)# inner-priority-trust enable
Hostname(config-if)#end
```

Related Commands

Command	Description
show inner-priority-trust	N/A

Platform Description N/A

8.8 l2protocol-tunnel

Use this command to set the dot1q-tunnel port to receive L2 protocol message. Use the **no** or **default** form of this command to disable this function.

l2protocol-tunnel stp
no l2protocol-tunnel stp
default l2protocol-tunnel stp

Parameter Description

Parameter	Description
stp	Receives stp message.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide If the STP and GVRP packets need to be transparently transmitted, this function must be enabled in global configuration mode.

Configuration Examples The following example enables the function of receiving L2 protocol gvrp and stp.

```
Hostname#configure
Hostname(config)# l2protocol-tunnel stp
Hostname(config)#end
```

Related Commands

Command	Description
show l2protocol-tunnel stp	N/A

Platform Description N/A

8.9 l2protocol-tunnel enable

Use this command to enable transparent transmission of L2 protocol message. Use the **no** or **default** form of this command to restore the default setting.
l2protocol-tunnel stp enable
no l2protocol-tunnel stp enable

Parameter Description

Parameter	Description
stp	Transparently transmits stp message.

Defaults It is disabled by default.

Command Mode Intereface configuration mode.

Usage Guide If this function is enabled in global and interface configuration modes, STP packets can be transparently transmitted after the bridge-frame forwarding protocol bpdu command is enabled in global configuration mode.

Configuration Examples 1: The following example enables transparent transmission of L2 protocol message:

```
Hostname# configure terminal
Hostname(config)# interface fa 0/1
Hostname(config-if)# l2protocol-tunnel stp enable
Hostname(config-if)#end
```

Related Commands

Command	Description
show l2protocol-tunnel stp	N/A

Platform Description N/A

8.10 l2protocol-tunnel tunnel-dmac

Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages. Use the **no** or **default** form of this command to restore the default setting.
l2protocol-tunnel stp tunnel-dmac *mac-address*
no l2protocol-tunnel stp tunnel-dmac *mac-address*
default l2protocol-tunnel stp tunnel-dmac *mac-address*

Parameter Description

Parameter	Description
stp	Sets the STP transparent transmission address.

Defaults The first three bytes of the address are 01d0f8 and the last three bytes are 000005 for **stp** and 000006 for **gvrp** by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the MAC address for the L2-protocol transparent transmission function on the interfacce:

```
Hostname# configure terminal
Hostname(config-if)# l2protocol-tunnel stp tunnel-dmac 011AA9 000005
Hostname(config-if)#end
```

Related Commands

Command	Description
show l2protocol-tunnel stp	N/A

Platform Description N/A

8.11 mac-address-mapping *x* source-vlan *src-vlan-list* destination-vlan *dst-vlan-id*

Use this command to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN. Use the **no** or **default** form of this command to restore the default setting.
mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
no mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
default mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*

Parameter Description

Parameter	Description
index-id	Policy ID of copying MAC addresses.
src-vlan-list	Source VLAN list of copying MAC addresses.
dst-vlan-id	Destination VLAN ID of copying MAC addresses.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example copies the MAC addresses dynamically-learned from the source VLANs 1-3 to the destination VLAN 5.

```
Hostname#configure
Hostname(config)# interface gigabitEthernet 0/2
Hostname(config-if)# mac-address-mapping 1 source-vlan  1-3 destination-vlan
5
Hostname(config-if)#end
```

Related Commands

Command	Description
show interface mac-address-mapping x	N/A

Platform N/A

Description

8.12 show dot1q-tunnel

Use this command to display whether dot1q-tunnel of interface is enabled or not.

show dot1q-tunnel [**interfaces** *intf-id*]

Parameter Description

Parameter	Description
intf-id	The specified interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays whether dot1q-tunnel of interface is enabled or not.

```
Hostname# show dot1q-tunnel
Ports   Dot1q-tunnel
-----   ---------
Gi0/1    Enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

8.13 show frame-tag tpid

Use this command to display the configuration of interface tpid.

show frame-tag tpid [**interfaces <***intf-id***>**]

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Any mode

Mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of interface tpid.

```
Hostname# show frame-tag tpid
Ports    tpid
-----  ---------
Gi0/1    0x9100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.14 show inner-priority-trust

Use this command to display whether the priority copy function is enabled.

show inner-priority-trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays whether the priority copy function is enabled.

```
Hostname# show inner-priority-trust
Port    inner-priority-trust
----    ----------
Gi0/1    enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

8.15 show interfaces dot1q-tunnel

Use this command to display the VLAN configuration on the dot1q-tunnel port.

show interfaces [*intf-Id*] **dot1q-tunnel**

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the VLAN configuration on the dot1q-tunnel port.

```
Hostname# show interfaces dot1q-tunnel
Interface: Gi0/3
Native vlan: 10
Allowed vlan list: 4-6, 10, 30-60
Tagged vlan list: 4, 6, 30-60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.16 show interfaces mac-address-mapping

Use this command to display the MAC address mapping configuration.

show interfaces mac-address-mapping

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the MAC address mapping configuration.

```
Hostname# show interfaces mac-address-mapping
Ports       Status    Index     Destination-VID Source-VID-list
----------- ---------- ---------- --------------- ------------------
Gi0/1       active    2         3             2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.17 show interfaces remark

Use this command to display the priority mapping configuration.

show interfaces [*intf-id*] **remark**

Parameter Description

Parameter	Description
intf-id	specifies an interface

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the priority mapping configuration.

```
Hostname# show interfaces remark
Ports         Type        From value  To value
------------ ----------- ----------- --------
Gi0/1         Cos-To-Cos  3           5
```

Field	Description
Ports	Port name.
Type	Type of priority mapping.

From value	Priority of inner tag
To value	Priority of outer tag after mapping.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.18 show interfaces vlan-mapping

Use this command to display the VLAN mapping configuration.

show interfaces vlan-mapping

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the VLAN mapping configuration.

```
Hostname# show interfaces vlan-mapping
Ports         Type    Status Destination-VID  Source-VID-list
------------  ------  -----  ---------------- ---------------
Gi0/1         in        active        5                3
Gi0/1         out       active        3                5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.19 show l2protocol-tunnel

Use this command to display transparent transmission configuration of L2 protocol.

show l2protocol-tunnel stp

Parameter Description

Parameter	Description
stp	Displays configuration of transparently transmitting stp protocol.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples 1: The following example displays transparent transmission configuration of L2 protocol.

```
Hostname# show l2protocol-tunnel stp
Destination mac : 01d0f8000005
L2protocol-tunnel: Stp Enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.20 show registration-table

Use this command to display vid add policy list of prorocol-based dot1q-tunnel port.

show registration-table [**interfaces** *intf-id*]

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays vid add policy list of prorocol-based dot1q-tunnel port.

Examples

```
Hostname# show registration-table
Ports      Type    Outer-VID  Inner-VID-list
---------   ------  ------- ------------------
Gi0/7        Add-outer  5          7-10,15,20-30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.21 show translation-table

Use this command to display vid modify policy list of prorocol-based access, trunk, hybrid port.

show translation-table [**interfaces** *intf-id*]

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays vid modify policy list of prorocol-based access, trunk, hybrid port.

```
Hostname# show translation-table
Ports       Type      Relay-VID  Old-local  Local\inner-VID-list
------------ ---------- ---------- ---------- ------------------
Gi0/7       Inner-CVID 8         N/A       10-20
Gi0/7       Local-SVID 1001      N/A       30-60
Gi0/7       In+Out     8         20        50
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.22 switchport dot1q-tunnel allowed vlan

Use this command to configure the allowed VLAN of dot1q-tunnel. Use the **no** or **default** form of this command to restore the default setting.

switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }

no switchport dot1q-tunnel allowed vlan

default switchport dot1q-tunnel allowed vlan

Parameter Description

Parameter	Description
add	Add allowed VLAN.
tagged	Tag-carried.
untagged	Not tag-carried.
v_list	vlan id list.
no	Remove the settings.

Defaults The default is **untagged** 1.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies vlan 3-6 of dot1q-tunnel port as allowed VLAN and outputting the frame with tag.

```
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if)#switchport dot1q-tunnel allowed vlan tagged 3-6
Hostname(config)#end
```

Related Commands

Command	Description
show interface dot1q-tunnel	N/A

Platform Description N/A

8.23 switchport dot1q-tunnel native vlan

Use this command to configure the default vlan id of dot1q-tunnel. Use the **no** or **default** form of this command to restore the default setting.

switchport dot1q-tunnel native vlan *vid*

no switchport dot1q-tunnel native vlan

default switchport dot1q-tunnel native vlan

Parameter Description

Parameter	Description
vid	Configures default vlan id.

Defaults The default is VLAN 1.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies default VLAN of dot1q-tunnel port as 8.

```
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if)#switchport dot1q-tunnel native vlan 8
Hostname(config)#end
```

Related Commands

Command	Description
show interface dot1q-tunnel	N/A

Platform Description N/A

8.24 switchport mode dot1q-tunnel

Use this command to configure the interface as the dot1q-tunnel interface. Use the **no** or **default** form of this command to restore the default setting.

switchport mode dot1q-tunnel

no switchport mode

default switchport mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults The interface is not a tunnel port by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the interface as the dot1q-tunnel interface.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if)# switchport mode dot1q-tunnel
Hostname(config)# end
```

Related Commands

Command	Description
show vlan	N/A

Platform Description N/A

9 ERPS Commands

9.1 associate sub-ring

Use this command to associate the ethernet ring with its sub-rings.

associate sub-ring raps-vlan *vlan-list*

no associate sub-ring raps-vlan *vlan-list*

Parameter Description

Parameter	Description
vlan-list	Sub-rings' R-APS VLAN.

Defaults By default, Ethernet ring is not associated with its sub-rings.

Command Mode ERPS configuration mode.

Usage Guide You need to configure this command on all nodes of the Ethernet ring, so as to transmit its sub-ring's ERPS protocol packets in the Ethernet ring.

Configuring the association is mainly to make the sub-ring's protocol packets transmit in the Ethernet ring. Users can also adopt the configuration command provided by the VLAN module to configure elaborately the VLAN and the relation between ports and VLAN, so as to transmit the sub-ring's protocol packets in other Ethernet rings and not leak the packets to the user network.

Configuration Examples The following example associates the Ethernet sub-ring with other Ethernet rings:

#Enter the privileged EXEC mode

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure the link mode of the Ethernet ring port and the default VLAN.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# interface fastEthernet 0/2
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
```

Enter the erps configuration mode.

```
Hostname(config)# erps raps-vlan 4093
```

#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Hostname(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet
```

```
0/2
```

Configure the Ethernet subring

```
Hostname(config)# erps raps-vlan 100
Hostname(config)# interface fastEthernet 0/3
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# erps raps-vlan 100
Hostname(config-erps100)#  ring-port west fastEthernet 0/3 east
virtual-channel
Hostname(config-if)# exit
```

Associate the subring with other Ethernet rings.

```
Hostname(config)# erps raps-vlan 4093
Hostname(config-erps4093)#  associate sub-ring raps-vlan 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.2 erps enable

Use this command to enable/disable the ERPS function in the global configuration mode.

erps enable

no erps enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Global configuration mode.

Usage Guide The ERPS protocol of the specified ring will begin running truly only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled.

Configuration Examples The following example enables the ERPS protocol globally:

```
# Enter the privileged EXEC mode
```

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
# Enable the ERPS function globally.
Hostname(config)# erps enable
```

```
# Enter the ERPS configuration mode
Hostname(config)# erps raps-vlan 4093
```

```
# Enable the ERPS function for the specified ring.
Hostname(config-erps4093)#  state enable
```

Related Commands

Command	Description
state enable	After entering the ERPS configuration mode of the specified ring, configure this command to enable the ERPS protocol of this specified ring.

Platform Description N/A

9.3 erps monitor link-state by oam

Use this command to configure the method of monitoring the ERPS link state.

erps monitor link-state by oam vlan *vlan-id*

no erps monitor link-state by oam

Parameter Description

Parameter	Description
vlan-id	Indicates the VLAN that monitors link state.

Defaults By default, it adopts the directly monitoring the link physical state (up or down) rather than the oam method.

Command Mode Global configuration mode.

Usage Guide For the link state monitoring, use the method of directly monitoring the link physical state (up or down), also monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link by the OAM. By default, the former is adopted. If the OAM method is used, the inefficient link state monitoring may cause the convergence time longer when the topology changes.

Configuration Examples The following example configures the method of monitoring the link state.

```
# Enter the privileged EXEC mode.
```

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

# Configure the method of monitoring the link state.
Hostname(config)# erps monitor link-state by oam vlan 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.4 erps raps-vlan

Use this command to configure the R-APS VLAN of Ethernet ring.

erps raps-vlan *vlan-id*

no erps raps-vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	R-APS VLAN ID

Defaults No R-APS VLAN is configured.

Command Mode Global configuration mode.

Usage Guide The R-APS VLAN must be the VLAN that is not used on the device. Cannot set the VLAN1 to the R-APS VLAN.

The same Ethernet ring of different devices needs the same R-APS VLAN.

If you want to transparently transmit the ERPS protocol packets on a device without the ERPS function configured, make sure that only the two ports connected to the Ethernet ring on this device allow the R-APSA VLAN packets corresponding to this ERPS ring passing through. Otherwise, the other VLAN packets may enter the R-APS VLAN through the transparent transmission, causing the shock to the ERPS ring.

Configuration Examples

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

#Configure the R-APS VLAN globally.
Hostname(config)# erps raps-vlan 4093
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.5 protected-instance

Use this command to configure the VLAN protected by the Ethernet ring to implement the load balance function.

protected-instance *instance-id-list*

no protected-instance

Parameter Description

Parameter	Description
instance-id-list	Instance protected by this Ethernet ring. (The VLANs corresponding to these instances are the VLANs protected by the Ethernet ring.)

Defaults By default, all VLANs are protected.

Command Mode EPRS configuration mode.

Usage Guide The protected VLAN consists of the R-APS VLAN of this Ethernet ring and the data VLAN protected by this Ethernet ring.

Configuration Examples Suppose that the ERP1 and ERP2 are configured on the switch to implement the load balance. The R-APS VLAN of the ERPS1 is 100, the protected data VLAN is in the range of 1 to 99 and 101-2000, the R-APS VLAN of the ERPS2 is 4093, and the protected data VLAN is in the range of 2001 to 4092 and 4094. Configuration for the load balance is shown as below:

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
# Configure the VLAN configured by the ERP1.
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-erps100)#protected-instance 1
```

```
# Configure the VLAN configured by the ERP2.
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-erps4093)#protected-instance 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.6 ring-port

Use this command to configure the ERPS ring.

ring-port west { *interface-name1* | **virtual-channel** } **east** { *interface-name2* | **virtual-channel** }

no ring-port

Parameter Description

Parameter	Description
interface-name1	Name of the West port.
interface-name2	Name of the East port.

Defaults No ERPS ring is configured.

Command Mode EPRS configuration mode.

Usage Guide 1) After adding the port to the ERP ring, the trunk attribute of the port is not allowed to be modified any more.

2) If the ring port is configured on the virtual-channel, this ring will be considered as a sub-ring.

3) Ports running the ERPS do not participate in the STP computing. ERPS, RERP and REUP do not share the port.

Configuration Examples The following example is for the ERPS ring.

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
# Configure the link mode of the Ethernet ring port and the default VLAN.
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# interface fastEthernet 0/2
```

```
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
```

```
# Enter the ERPS configuration mode.
Hostname(config)# erps raps-vlan 4093
```

```
#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Hostname(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

Related Commands

Command	Description
state enable	Enable the ERPS protocol of the specified ring in the ERPS mode of the specified ring.
sub-ring associate raps-vlan *vlan-id*	Establish the association between the subring and other Ethernet rings in the subring ERPS configuration mode.

Platform Description N/A

9.7 rpl-port

Use this command to configure the RPL port and RPL owner.

rpl-port { **west** | **east** } [**rpl-owner**]

no rpl-port

Parameter Description

Parameter	Description
west	Name of the West port.
east	Name of the East port.

Defaults No RPL port and RPL owner are configured.

Command Mode EPRS configuration mode.

Usage Guide Up to one RPL link and one RPL owner node are needed and configurable for each ring.

Configuration Examples The following example configures the RPL port and RPL owner.

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
# Configure the link mode of the Ethernet ring port and the default VLAN.
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# interface fastEthernet 0/2
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
```

```
# Enter the ERPS configuration mode.
Hostname(config)# erps raps-vlan 4093
```

```
# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Hostname(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet
0/2
```

```
# Specify the port where the RPL link is and the RPL owner.
Hostname(config-erps4093)#  rpl-port west rpl-owner
```

Related Commands

Command	Description
ring-port west { *interface-name1* | **virtual-channel** } **east** { *interface-name2* | **virtual-channel** }	Configure the specified ERP ring in the ERPS configuration mode of the specified ring.
state enable	Enable the ERPS protocol of the specified ring in the ERPS configuration mode of the specified ring.

Platform Description N/A

9.8 show erps

Use this command to show the parameters and states of the ERPS.

show erps [{ **global** | **raps_vlan** *vlan-id* [**sub-ring**] }]

Parameter Description

Parameter	Description
global	Displays global ERPS information.
raps_vlan *vlan-id*	Displays specified ERPS information.
sub-ring]	Displays specified sub ring information.

Defaults N/A

Command Mode Any mode.

Usage Guide N/A

Configuration Examples The following example shows the use of this command.

```
Hostname# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by           : Not Oam
-------------------------------------------
R-APS VLAN                       : 4092
Ring Status                      : Enabled
West Port                        : Gi 0/5 (Blocking)
East Port                        : Gi 0/7 (Forwarding)
RPL Port                         : West Port
RPL Port Blocked VLAN       : All
RPL Owner                        : Enabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
-------------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Virtual Channel
East Port                        : Gi 0/10 (Forwarding)
RPL Port                         : None
RPL Port Blocked VLAN           : All
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
Guard Time                       : 500 milliseconds
WTR Time                         : 5 minutes
Current Ring State               : Idle
-------------------------------------------
R-APS VLAN                       : 4094
Ring Status                      : Enabled
West Port                        : Virtual Channel
East Port                        : 12 (Forwarding)
RPL Port                         : None
RPL Port Blocked VLAN           : All
RPL Owner                        : Disabled
Holdoff Time                     : 0 milliseconds
```

```
Guard Time                      : 500 milliseconds
WTR Time                        : 5 minutes
Current Ring State              : Idle

Hostname# show erps raps_vlan 4093 sub-ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs    TC Propagation State
--------------------    --------------------
100                        Enable
200                        Enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.9 state enable

Use this command to enable/disable the specified R-APS ring.

state enable

no state enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode EPRS configuration mode.

Usage Guide Only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled, the ERPS protocol of the specified ring will begin truly running.

Configuration Examples The following example enables the specified ERPS ring:

```
#Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

#Configure the link mode of the Ethernet ring port and the default VLAN.
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# switchport mode trunk
```

```
Hostname(config-if)# exit
Hostname(config)# interface fastEthernet 0/2
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit

# Enter the ERPS configuration mode.
Hostname(config)# erps raps-vlan 4093

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Hostname(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet
0/2

# Enable the ERPS function for the specified ring.
Hostname(config-erps4093)#state enable

# Enable the global ERPS function.
Hostname(config-erps4093)# exit
Hostname(config)# erps enable
```

Related Commands

Command	Description
erps enable	Enable the global ERPS protocol.

Platform Description N/A

9.10 sub-ring tc-propagation

Use this command to specify the devices corresponding to the crossing node on the crossing ring whether to send out the notification when the subring topology changes.

sub-ring tc_propagation enable

no sub-ring tc_propagation

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the topology changing notification is not sent.

Command Mode EPRS configuration mode.

Usage Guide This command is just needed to be configured on the crossing nodes on the crossing ring.

Configuration Examples The following example is configured when the subring topology changes.

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

#Configure the link mode of the Ethernet ring port and the default VLAN.
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# interface fastEthernet 0/2
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit

# Enter the ERPS configuration mode.
Hostname(config)# erps raps-vlan 4093

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Hostname(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet
0/2

#Configure the Ethernet subring.
Hostname(config)# erps raps-vlan 100
Hostname(config)# interface fastEthernet 0/3
Hostname(config-if)# switchport mode trunk
Hostname(config-if)# exit
Hostname(config)# erps raps-vlan 100
Hostname(config-erps100)#  ring-port west fastEthernet 0/3 east
virtual-channel

# Associate the subring with other Ethernet rings.
Hostname(config-erps100)#  sub-ring associate raps-vlan 4093

# Enable the topology changing notification for the subring.
Hostname(config-erps100)#  sub-ring tc-propagation enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.11 timer

Use this command to configure the timer of the ERPS protocol.

timer { **holdoff-time** *interval1* | **guard-time** *interval2* | **wtr-time** *interval3* }

no timer { **holdoff-time** | **guard-time** | **wtr-time** }

Parameter Description

Parameter	Description
holdoff-time *interval1*	Value of the Holdoff timer in 100 milliseconds, the valid range is 0 to 100.
guard-time *interval2*	Value of the Guard timer in 10 milliseconds, the valid range is 1 to 200.
wtr-time *interval3*	Value of the WTR in minute, the valid range is 5 to 12.

Defaults

Holdoff timer: 0.

Guard timer: 500 milliseconds.

WTP timer: 5 seconds.

Command Mode

EPRS configuration mode.

Usage Guide

Holdoff timer: This timer is used to avoid the ERPS from topology swithcingswitching continuously due to the link intermittent fault. With this timer configured, if the link fault is detected, the ERPS does not perform the topology switching immediately until the timer times out and the link fault is verified.

Guard timer: This timer is used to prevent the device receiving the timed-out R-APS messages. When the device detects the recovery from failure of the link, it sends out the message of link recovery and starts up the Guard timer. Before the Guard times out, except for the flush packets indicating the subring topology change, other packets are discarded directly without being handled.

WTR (Wait-to-restore) timer: This timer is only valid for the RPL owner device. It is mainly used to prevent the RPL owner making the erroneous judgment to the ring network status. When the RPL detects the fault recovery, it does not perform the topology switching immediately until the WTR times out and the Ethernet ring indeed recovers from the fault. If the ring network fault is checked again before the WTR times out, then the WTR timer will be canceled and topology switching will be not executed any longer.

Configuration Examples

The following example configures the timer of the ERPS protocol.

```
# Enter the privileged EXEC mode.
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
# Enter the ERPS configuration mode.
Hostname(config)# erps raps-vlan 4093

# Configure the protocol timer.
Hostname(config-erps4093)#  timer holdoff-time 10
```

```
Hostname(config-erps4093)#  timer guard-time 10
Hostname(config-erps4093)#  timer wtr-time 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

IP Address & Application Commands

1. IP Address/Service Commands
2. ARP Commands
3. IPv6 Commands
4. DHCP Commands
5. DNS Commands

6.FTP Server Commands

7.FTP Client Commands

8. TFTP Client Commands
9. Network Connectivity Test Tool Commands
10. TCP Commands
11. IPv4/IPv6 REF Commands

1 IP Address/Service Commands

1.1 ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask* [**secondary**]

no ip address [*ip-address network-mask* [**secondary**]]

Parameter Description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
secondary	Secondary IP address

Defaults No IP address is configured for the interface by default.

Command Mode Interface configuration mode

Usage Guide The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The system software supports configuring multiple IP address for an interface, in which one is the primary IP address and others are the secondary IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

A network hasn't enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.

Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.

Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

Configuration Examples The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
```

The following example configures the default gateway as 10.10.10.254.

```
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
```

Related Commands

Command	Description
show interface	Displays detailed information of the interface.

Platform Description N/A

1.2 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss

Parameter Description

Parameter	Description
ip-address	Broadcast address of IP network

Defaults The default IP broadcast address is 255.255.255.255.

Command Interface configuration mode.

Mode

Usage Guide At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The system software can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.

Configuration Examples The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip broadcast-address  0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter Description

Parameter	Description
access-list-number	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically

the broadcast packet whose destination IP address is all “1”), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, the system will discard the directed broadcast packets received from the directly connected network.

Configuration Examples

The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip directed-broadcast
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.4 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

ip icmp error-interval DF milliseconds [*bucket-size*]

no ip icmp error-interval DF *milliseconds* [*bucket-size*]

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

ip icmp error-interval milliseconds [bucket-size]

no ip icmp error-interval *milliseconds* [*bucket-siz*]

Parameter Description

Parameter	Description
milliseconds	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
bucket-size	The number of tokens in the bucket, in the range is from 1 to

	200. The default is 10.

Defaults The default rate is 10 packets per 100 millisecond.

Command Mode Global configuration mode.

Usage Guide To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.

If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.

It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

Configuration Examples The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
Hostname(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Hostname(config)# ip icmp error-interval 1000 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 ip icmp timestamp

Use this command to enbale the device to return a Timestamp Reply. Use the **no** form of this command to disable returning of Timestamp Reply.

ip icmp timestamp

no ip icmp timestamp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example disables the device to return a Timestamp Reply.

```
Hostname(config)# no ip icmp timestamp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.6 ip mask-reply

Use this command to configure the system to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip mask-reply

no ip mask-reply

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode.

Usage Guide Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Configuration Examples The following example sets the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip mask-reply
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.7 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command is restore the default setting.

ip mtu *bytes*

no ip mtu

Parameter Description

Parameter	Description
bytes	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes

Defaults It is the same as the value configured in the interface command **mtu** by default.

Command Mode Interface configuration mode.

Usage Guide If an IP packet is larger than the IP MTU, the system will segment this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Configuration Examples The following iexample sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip mtu 512
```

Related Commands

Command	Description
mtu	Sets the MTU value of an interface.

Platform Description N/A

1.8 ip redirects

Use this command to allow the system to send an ICMP redirection message in the interface configuration mode. Use the **no** form of this command to disable this function.

ip redirects

no ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.
By default, the system software enables ICMP redirection.

Configuration Examples The following example disables ICMP redirection for the fastEthernet 0/1 interface.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# no ip redirects
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.9 ip source-route

Use this command to allow the system to process an IP packet with source route information in global configuration mode. Use the **no** form of this command to disable this function.
ip source-route
no ip source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide The system supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.
By default, the system software supports the IP source route feature.

Configuration Examples The following example disables the IP source route.

```
Hostname(config)# no ip source-route
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.10 ip ttl

Use this command to set the TTL value of the unicast packet. Use the **no** form of this command to restore the default setting.

ip ttl *value*

no ip ttl

Parameter Description	Parameter	Description
	value	Sets the TTL value of the unicast packet, in the range from 0 to 255.

Defaults The default is 64.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the TTL value of the unicast packet to 100.

```
Hostname(config)# ip ttl 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.11 ip ttl-expires enable

This command is used to enable notifications of expired TTL. Use the **no** form of this command to disable this function.

ip ttl-expires enable

no ttl-expires enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, notifications are enabled to indicate expired TTL.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example disables notifications indicating expired TTL.

```
Hostname(config)# no ttl-expires enable
```

Platform Description N/A

1.12 ip unreachables

Use this command to allow the system to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

ip unreachables

no ip unreachables

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide The system software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.

The system software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.

This command influences all ICMP destination unreachable messages.

Configuration Examples The following example disables sending ICMP destination unreachable message on FastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# no ip unreachables
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.13 show ip interface

Use this command to display the IP status information of an interface.

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type	Specifies interface type.
interface-number	Specifies interface number.
brief	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide When an interface is available, the system will create a direct route in the routing table. The interface is available in the system software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the system software will remove the appropriate direct route from the routing table.

If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as “UP”. If only the physical line is available, the interface status will be shown as “UP”.

The results shown may vary with the interface type, because some contents are the interface-specific options

Configuration Examples The following exmaple displays the output of the **show ip interface brirf command**.

```
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
```

Description of fields:

Field	Description
Status	Link status of an interface. The value can be **up**, **down**, or **administratively down**.
Protocol	IPv4 protocol status of an interface.

The following example displays the output of the **show ip interface vlan** command.

```
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
 DHCP relay is: OFF
 Fast switch is: ON
 Help address is:
 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
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are “UP”.
IP interface type is:	Show the interface type, such as broadcast, point-to-point,

	etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachabled is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fash switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: Request packet: Reply packet: Unknown packet:	Show the total number of ARP packets received on the interface, including: ARP request packet ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet

Related Commands	**Command**	**Description**
	N/A.	N/A.

Platform Description N/A.

1.14 show ip packet queue

Use this command to display the statistics of IP packet queues.

show ip packet queue

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the statistics of IP packet queues.

Products do not support the VRF parameter. The following example is for reference purpose. Please take the actual product as the standard.

```
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.
```

Field	Description
IP packet receive queue	Statistics of received packets
Discards	Statistics of discarded packets
Sent packets	Statistics of sent packets
ICMP error queue	Statistics of ICMP error packets

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.15 show ip packet statistics

Use this command to display the statistics of IP packets.

show ip packet statistics [**total** | *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name
total	Displays the total statistics of all interfaces.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output of this command.

```
R1#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
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.16 show ip raw-socket

Use this command to display IPv4 raw sockets.

show ip raw-socket [*num*]

Parameter Description	Parameter	Description
	num	Protocol.

Defaults N/A.

Command Mode Priviledged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays all IPv4 raw sockets.

```
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
```

Field Description

Field	Description

Number	Number
Protocol	Protocol
Process name	Process name
Total	Total number

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.17 show ip sockets

Use this command to display all IPv4 sockets.

show ip sockets

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following displays all IPv4 sockets.

```
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        mpls.elf           DGRAM      UDP        0.0.0.0:3503   0.0.0.0:0
*
10       rds_other_th       DGRAM      UDP        0.0.0.0:3799   0.0.0.0:0
*
11       rg-snmpd           DGRAM      UDP        0.0.0.0:14800  0.0.0.0:0
*
12       rg-sshd            STREAM     TCP        0.0.0.0:22     0.0.0.0:0
LISTEN
13       rg-telnetd         STREAM     TCP        0.0.0.0:23     0.0.0.0:0
LISTEN
14       wbard              STREAM     TCP        0.0.0.0:4389   0.0.0.0:0
LISTEN
15       wbard              STREAM     TCP        0.0.0.0:7165   0.0.0.0:0
LISTEN
Total: 15
```

Field Description

Field	Description
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.18 show ip udp

Use this command to display IPv4 UDP sockets.

show ip udp [**local-port** *num* | **peer-port** *port-number*]

Use this command to display IPv4 UDP socket statistics.

show ip udp statistics

Parameter Description

Parameter	Description
local-port *num*	Local port number
peer-port *port-number*	Peer port number

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays all IPv4 UDP sockets.

```
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           rg-snmpd
3      0.0.0.0:2000         0.0.0.0:0           wbav2
4      0.0.0.0:3333         0.0.0.0:0           vrrp_plus.elf
5      0.0.0.0:3503         0.0.0.0:0           mpls.elf
6      0.0.0.0:3799         0.0.0.0:0           rds_other_th
7      0.0.0.0:14800        0.0.0.0:0           rg-snmpd
```

Field Description

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2 ARP Commands

2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the **no** form of this command to restore the default setting.

arp *ip-address MAC-address type* [**alias**]

no arp *ip-address MAC-address type* [**alias**]

Parameter Description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is arpa for the Ethernet interface.

Defaults There is no static mapping record in the ARP cache table by default.

Command Mode Global configuration mode.

Usage Guide The system finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table.

Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

Configuration Examples The following example sets an ARP static mapping record for a host in the Ethernet.

```
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands

Command	Description
clear arp-cache	Clears the ARP cache table

Platform Description N/A

2.2 arp anti-ip-attack

For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learning). Sending large number of this message to the CPU will influence the other tasks of

the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messages with that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address in hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possible to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the *num* parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function. Use the **arp anti-ip-attack** command to set the parameter or disable this function. Use the **no** form of this command to restore the default setting.

arp anti-ip-attack *num*

no arp anti-ip-attack

Parameter Description

Parameter	Description
num	The number of the IP message to trigger the ARP to discarded entry in the range from 0 to 100. 0 stands for disabling the arp anti-ip-attack function.

Defaults By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.

Command Mode Global configuration mode.

Usage Guide The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the **arp anti-ip-attack *num*** could be smaller. If not, in order to preferential ensure the use of the normal routing, the *num* could be larger or disable this function.

Configuration Examples The following example sets the IP message number that triggers ARP to discarding entry as 5.

```
Hostname(config)# arp anti-ip-attack 5
```

The following example disables the ARP anti-ip-attack function.

```
Hostname(config)# arp anti-ip-attack 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 arp cache interface-limit

Use this command to set the maximum number of ARP learned on the interface.

Use the **no** form of this command to restore the default setting.

arp cache interface-limit *limit*

no arp cache interface-limit

Parameter Description

Parameter	Description
limit	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to 512. 0 indicates that the number is not limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent ARP attacks from generating ARP entries to consume memory. *limit* must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the maximum number of ARP learned on the interface to 300.

```
Hostname(config)# interface gi 0/0
Hostname(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

The following example restores the default setting.

```
Hostname(config)# interface gi 0/0
Hostname(config-if-GigabitEthernet 0/0)# no arp any-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.4 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. Use the**no** form of this command to restore the default setting.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter Description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Configuration Examples The following example sets to send one free ARP request to SVI 1 per second.

```
Hostname(config)# interface vlan 1
Hostname(config-if)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to SVI 1.

```
Hostname(config)# interface vlan 1
Hostname(config-if)# no arp gratuitous-send
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.5 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.

arp retry interval *seconds*

no arp retry interval

Parameter Description

Parameter	Description
seconds	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.

Defaults The default is 1.

Command Mode Global configuration mode.

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Configuration The following example sets the retry interval of the ARP request as 30 seconds.

Examples

```
Hostname(config)# arp retry interval 30
```

Related Commands

Command	Description
arp retry times	Number of times for retransmitting an ARP request message.

Platform Description N/A

2.6 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the **no** form of this command to restore the default setting.

arp retry times *number*

no arp retry times

Parameter Description

Parameter	Description
number	The times of sending the same ARP request in the range from 1 to100.When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Defaults The default is 5.

Command Mode Global configuration mode.

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Configuration Examples The following example sets the local ARP request not to be retried.

```
Hostname(config)# arp retry times 1
```

The following example sets the local ARP request to be retried for one time.

```
Hostname(config)# arp retry times 2
```

Related Commands

Command	Description
arp retry interval	Interval for retransmitting an ARP request message

Platform Description N/A

2.7 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. Use the **no** form of this command to restore the default setting.

arp timeout *seconds*

no arp timeout

Parameter Description

Parameter	Description
secondsv	The timeout is in the range from 0 to 2147483 in the unit of seconds.

Defaults The default is 3600.

Command Mode Interface configuration mode

Usage Guide The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Configuration Examples The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# arp timeout 120
```

Related Commands

Command	Description
clear arp-cache	Clears the ARP cache list.
show interface	Displays the interface information.

Platform Description N/A

2.8 arp trust-monitor enable

Use this command to enable egress gateway trusted ARP. Use the **no** form of this command to restore the default setting.

arp trust-monitor enable

no arp trust-monitor enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.

Configuration Examples The following example enables egress gateway trusted ARP.

```
Hostname(config)# interface gi 0/0
Hostname(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

The following example disables engress gateway trusted ARP.

```
Hostname(config)# interface gi 0/0
Hostname(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.9 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

arp unresolve *number*

no arp unresolve

Parameter Description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range from 1 to 1000.

Defaults The default is the ARP table size supported by the device.

Command Mode Global configuration mode.

Usage Guide If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

Configuration Examples The following example sets the maximum number of the unresolved items to 500.

```
Hostname(config)# arp unresolve 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.

clear arp-cache [**trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

Parameter Description

Parameter	Description
ip	Deletes ARP entries of the specified IP address. If *trusted* value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
mask	Deletes ARP entries in a subnet mask. If *trusted* value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
interface *interface-name*	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

Command Mode Privileged EXEC mode

Usage Guide This command can be used to refresh an ARP cache table.

On a NFPP-based (Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Configuration Examples The following example deletes all dynamic ARP mapping records.

```
Hostname# clear arp-cache
```

The following deletes the dynamic ARP entry 1.1.1.1.

```
Hostname# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SVI1.

```
Hostname# clear arp-cache interface Vlan 1
```

Related Commands	Command	Description
	arp	Adds a static mapping record to the ARP cache table.

Platform Description N/A

2.11 ip proxy-arp

Use this command to enable ARP proxy function on the interface. Use the **no** form of this command to restore the default setting.

ip proxy-arp

no ip proxy-arp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, ARP proxy is disabled.

Command Mode Interface configuration mode.

Usage Guide Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Configuration Examples The following example enables ARP on FastEthernet port 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip proxy-arp
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.12 local-proxy-arp

Use this command to enable local proxy ARP on the SVI interface. Use the **no** form of this command to restore the default setting.

local-proxy-arp

no local-proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide With local proxy ARP enabled, the device helps a host to obtain MAC addresses of other hosts on the subnet. If the device enables switchport protected, users on different ports are segregated on layer 2. After local proxy ARP is enabled, the device serves as a proxy to send a response after receiving an ARP request. The ARP response contains a MAC address which is the device's Ethernet MAC address, realizing communication between different hosts through L3 routes.

Configuration Examples The following example enables local proxy ARP on VLAN1.

```
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# local-proxy-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

show arp [*interface-type interface-number* | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the ARP entry of a specified Layer-2 or Layer-3 port.
ip	Displays the ARP entry of the specified IP address. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
mask	Displays the ARP entries of the network segment included within the mask. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
static	Displays all the static ARP entries.

complete	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.
mac-address	Displays the ARP entry with the specified mac address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output result of the **show arp** command:

```
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 meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following example displays the output result of show arp 192.168.195.68

```
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 the output result of **show arp** 192.168.195.0 255.255.255.0

```
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 output result of **show arp** 001a.a0b5.378d

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.14 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

show arp counter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output result of the **show arp counter** command:

```
Hostname#sho arp counter
ARP Limit:              75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1  incomplete: 0)
Total:                  1
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

2.15 show arp detail

Use this command to display the details of the Address Resolution Protocol (ARP) cache table.

show arp detail [*interface-type interface-number* | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the ARP of the layer 2 port or the layer 3 interface.
ip	Displays the ARP entry of the specified IP address.
ip mask	Displays the ARP entries of the network segment included within the mask.
mac-address	Displays the ARP entry of the specified MAC address.
static	Displays all the static ARP entries.
complete	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the ARP details, such as the ARP type (Dynamic, Static, Local), the information on the layer2 port.

If you enter a *min_value g*reater than *max_value*, no error message is prompted. Instead, ARP entries corresponding to the subvlan are displayed.

Configuration Examples The following example displays the output result of the **show arp detail** command:

```
Hostname# show arp detail
IP Address      MAC Address    Type    Age(min) Interface  Port
192.168.101.1   0074.9c95.d9f9 Dynamic  8       VLAN 1    Gi0/1
192.168.101.5   00d0.f822.33d1 Local    --      VLAN 1    --
Total number of ARP entries: 2
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
IP Address	IP address corresponding to the hardware address

MAC Address	hardware address corresponding to the IP address
Age (min)	Age of the ARP learning, in minutes
Port	Layer2 port associated with the ARP
Type	ARP type, includes the Static, Dynamic, Trust,Local
Interface	Layer 3 interface associated with the IP addresses

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 show arp packet statistics

Use this command to display the statistics of ARP packets.

show arp packet statistics [*interface-name*]

Parameter Description

Parameter	Description
interface-name	Displays the statistics of ARP packets on the specified interface.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output information of the command.

```
Hostname#show arp packet statistics
Interface           Received  Received Received  Sent     Sent
Name               R
equests  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
```

Description of fields:

Field	description
Received Requests	Number of received ARP requests
Received Replies	Number of received ARP response messages
Received Others	Number of other received ARP packets
Sent Requests	Number of sent ARP requests
Sent Replies	Number of sent ARP requests

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A

2.17 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

show arp timeout

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide N/A.

Configuration Examples The following example displays the output of the **show arp timeout** command:

```
Hostname# show arp timeout
Interface arp timeout(sec)
---------------------- ----------------
VLAN 1  3600
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A

2.18 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp

Parameter Description	**Parameter**	**Description**
	N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output of **show ip arp**:

```
Hostname# show ip arp
Protocol Address Age(min)Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0
Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0
Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Related Commands	**Command**	**Description**
	N/A.	N/A.

Platform N/A

Description

3 IPv6 Commands

Note:

"Router" in this chapter refers to the network device that supports the routing function. These network devices can be Layer 3 switches, routers, firewalls, etc.

3.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

clear ipv6 neighbors [*interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command does not clear all the dynamic neighbors on authentication VLAN.
Note that the static neighbors will not be cleared.

Configuration Examples The following example clears the dynamic IPv6 neighbors.

```
Hostname# clear ipv6 neighbors
```

The following example clears dynamic IPv6 neighbors on the interface gigabitEthernet 0/1.

```
Hostname# clear ipv6 neighbors gigabitEthernet 0/1
```

Related Commands

Command	Description
ipv6 neighbor	Configures the neighbor.
show ipv6 neighbors	Displays the neighbor information.

Platform Description N/A

3.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

ipv6 address ipv6-address/prefix-length

ipv6 address *ipv6-prefix/prefix-length* **eui-64**
ipv6 address *prefix-name sub-bits/prefix-length* [**eui-64**]
no ipv6 address
no ipv6 address *ipv6-address/prefix-length*
no ipv6 address *ipv6-prefix/prefix-length* **eui-64**
no ipv6 address *prefix-name sub-bits/prefix-length* [**eui-64**]

Parameter Description

Parameter	Description
iipv6-prefix	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
ipv6-address	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
prefix-name	The general prefix name. Use the specified general prefix to generate the interface address.
sub-bits	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

Defaults N/A

Command Mode Interface configuration mode

Usage Guide When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.
The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.
If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.
no ipv6 address *ipv6-prefix***/***prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix***/***prefix-length* **eui-64**.

Configuration Examples

```
Hostname(config-if)# ipv6 address 2001:1::1/64
Hostname(config-if)# no ipv6 address 2001:1::1/64
```

```
Hostname(config-if)# ipv6 address 2002:1::1/64 eui-64
Hostname(config-if)# no ipv6 address 2002:1::1/64 eui-64
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.3 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to restore the default setting.

ipv6 address autoconfig [**default**]

no ipv6 address autoconfig

Parameter Description	Parameter	Description
	default	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the **default** keyword

Defaults N/A

Command Mode Interface configuration mode

Usage Guide The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

Use the **no ipv6 address autoconfig** command to delete the IPv6 address.

Configuration Examples

```
Hostname(config-if)# ipv6 address autoconfig default
Hostname(config-if)# no ipv6 address autoconfig
```

Related Commands	Command	Description
	ipv6 address ipv6-*prefix/prefix-length* [**eui-64**]	Configures the IPv6 address for the interface manually.

Platform Description N/A

3.4 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to restore the default setting.

ipv6 enable

no ipv6 enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

Configuration Examples

```
Hostname(config-if)# ipv6 enable
```

Related Commands

Command	Description
show ipv6 interface	Displays the related information of an interface.

Platform Description N/A

3.5 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.
A general prefix could contain multiple prefixes.
These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

Configuration Examples The following example configures manually a general prefix as my-prefix.

```
Hostname(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related Commands

Command	Description
ipv6 address prefix-name sub-bits/prefix-length	Configures the interface address using the general prefix.
show ipv6 general-prefix	Displays the general prefix.

Platform Description N/A

3.6 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.
ipv6 hop-limit *value*
no ipv6 hop-limit

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is 64.

Command Mode Global configuration mode.

Usage Guide This command takes effect for the unicast messages only, not for multicast messages.

Configuration Examples

```
Hostname(config)# ipv6 hop-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the **no** form of this command to restore the default setting.

ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

no ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the **no** form of this command to restore the default setting.

ipv6 icmp error-interval *milliseconds* [*bucket-size*]

no ipv6 icmp error-interval *milliseconds* [*bucket-size*]

Parameter Description

Parameter	Description
milliseconds	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
bucket-size	Sets the number of tokens in the token bucket, in the range from 1 to 200.

Defaults The default *milliseconds* is 100 and *bucket-size* is 10.

Command Mode Global configuration mode

Usage Guide The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack,

If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and devices sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet.

For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

Configuration The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100

Examples per second.

```
Hostname(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second.

```
Hostname(config)# ipv6 icmp error-interval 1000 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

ipv6 mtu *bytes*

no ipv6 mtu

Parameter Description

Parameter	Description
bytes	MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500.

Defaults The default configuration is the same as the configuration of the **mtu** command.

Command Mode Interface configuration mode

Usage Guide If the size of an IPv6 packet exceeds the IPv6 MTU, the system software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.

Configuration Examples The following example sets the IPv6 MTU of the FastEthernet 0/1 interface to 1400 bytes.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ipv6 mtu 1400
```

Related Commands

Command	Description
mtu	Sets the MTU of an interface.

Platform Description This command cannot be used on Layer 2 devices.

3.9 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd cache interface-limit *value*

no ipv6 nd cache interface-limit

Parameter Description

Parameter	Description
value	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to 512. 0 indicates the number is not limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. *limit* must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the number of neighbors learned on the interface to 100.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd dad attempts value

no ipv6 nd dad attempts *value*

Parameter Description

Parameter	Description
value	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Defaults The default is 1.

Command Mode Interface configuration mode.

Usage Guide When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the ”tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Configuration Examples The following example configures sending three neighbor request messages when conflict detection is configured on the interface GigabitEthernet 0/1.

```
Hostname(config-if)# ipv6 nd dad attempts 3
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

3.11 ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.

ipv6 nd dad retry *value*

no ipv6 nd dad retry

Parameter Description

Parameter	Description
value	Sets the interval for address conflict detection, 60 seconds by default. Setting *value* to 0 indicates that the function is disabled.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the

conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

Configuration Examples The following example sets the interval for address conflict detection to 10s.

```
Hostname(config)# ipv6 nd dad retry 10
```

Platform Description N/A

3.12 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

Configuration Examples The following examples sets the “managed address configuration” flag bit of the RA message on the interface GigabitEthernet 0/1.

```
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd other-config-flag	Sets the flag for obtaining all information except IP address through stateful auto configuration.

Platform Description N/A

3.13 ipv6 nd max-opt

Use this command to configure the limit on the number of ND options to be processed by the device.
ipv6 nd max-opt *value*

Use the **no** form of this command to restore the default setting.
no ipv6 nd max-opt

Parameter Description

Parameter	Description
value	Number of ND options supported. The value range is 1-100.

Defaults The default value is 10.

Command Mode Global configuration mode

Default Level 14

Usage Guide You can use this command to configure the limit of ND options processed by the device, including source link layer address, MTU, redirection, prefixes.

Configuration Examples 1: The following example sets the limit of ND options processed by the device to 20.

```
Hostname(config)# ipv6 nd max-opt 20
```

Verification Run the **show running-config** command to view whether the configuration takes effect.

Prompt messages N/A

Common Errors N/A

Platform Description N/A

3.14 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore the default setting.
ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

Parameter Description	Parameter	Description
	milliseconds	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Defaults The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000 milliseconds (1 second).

Command mode Interface configuration mode.

Usage Guide The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

Configuration Examples

```
Hostname(config-if)# ipv6 nd ns-interval 2000
```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Platform Description N/A

3.15 ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The flag bit is not set by default.

Command mode Interface configuration mode.

Usage Guide With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

Configuration Examples

```
Hostname(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

3.16 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

ipv6 nd prefix { *ipv6-prefix*/*prefix-length* | **default** } [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | [**infinite** | *preferred-lifetime*]] [[**off-link**] [**no-autoconfig] | [preference** { *high* | *medium* | *low* }]] | [**no-advertise**]]

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** }

Parameter Description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. “/” shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at valid-date preferred-date	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicates that the prefix is always valid.
default	Sets the default prefix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicates that the RA prefix received by the host cannot be used for auto address configuration.
preference	Sets the routing priority. The values are high, medium, and low.

Defaults By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

valid-lifetime: 2592000s (30 days)

preferred-lifetime: 604800s (7 days),

The prefix is advertised and is used for on-link judgment and auto address configuration.

Command Interface configuration mode.

Mode

Usage Guide This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Configuration Examples The following example adds a prefix for SVI 1.

```
Hostname(config)# interface vlan 1
Hostname(config-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Hostname(config)# interface vlan 1
Hostname(config-if)# ipv6 prefix default no-autoconfig
```

Note:

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related Commands

Command	Description
show ipv6 interface	Displays the RA information of an interface.

Platform Description N/A

3.17 ipv6 nd ra dns server

Run this command to configure the router advertisement (RA) messages to suppress sending RDNSS addresses.

ipv6 nd ra dns server suppress

Run this command to configure the server IP address of DNS recursive resolution service in the RA message.

ipv6 nd ra dns server *ipv6-address* {*valid-lifetime* | **infinite**} **sequence** *number*

Run this command to configure the RA message to send RDNSS addresses.

no ipv6 nd ra dns server suppress

Run this command to remove the configured recursive DNS server address.

no ipv6 nd ra dns server *ipv6-address* {*valid-lifetime* | **infinite**} **sequence** *number*

Parameter Description

Parameter	Description
ipv6-address	IPV6 address, which must follow the address format defined in RFC4291. Each address field is separated by a colon. Each field takes 16 bits and is represented by a hexadecimal number.
suppress	Suppress RA message to carry the RDNSS option. The default is suppress.
valid-lifetime	The time that the host considers valid after receiving the RDNSS option advertised by the router. The value range is 0-4294967295. If it is set to 0, it means the RDNSS address is no longer used.
infinite	Means always valid.
number	The sequence, indicating the serial number of the same RDNSS option in the RA message.

Defaults By default, the RDNSS option of RA message is disabled.

Command Mode Interface configuration mode

Default Level 14

Usage Guide Run the **no ipv6 nd ra dns server suppress** command to enable the RA message to carry RDNSS option.

Run the **ipv6 nd ra dns server** *ipv6-address* {*valid-lifetime* | **infinite**} **sequence** *number* command to configure RDNSS option and parameter advertised in RA. On the same interface, only one option can be configured for the same sequence, and the same IPv6 address can only be used by one sequence. A valid life time of 0 means it is no longer used, and the value **infinite** means it is always valid. After the RDNSS option is configured, this option will be advertised through the RA message, and the RDNSS options in the RA message will be organized in sequence in descending order.

Configuration Examples 1: The following example enables RDNSS function on the interface VLAN 1 and configures RDNSS option.

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)# no ipv6 nd rad ns server suppress
```

```
Ruijie(config-if-VLAN 1)# ipv6 nd ra dns server 2018::1 infinite sequence 0
Ruijie(config-if-VLAN 1)# ipv6 nd ra dns server 2020::1 1000 sequence 1
```

2: The following example deletes a prefix on interface VLAN1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# no ipv6 nd ra dns server 2018::1 infinite sequence 0
Ruijie(config-if-VLAN 1)# no ipv6 nd ra dns server 2020::1 1000 sequence 1
```

Verification Run the **show ipv6 nd ra dns server** command to view the IP address of the server which provides the DNS recursive resolution service in the RDNSS in the RA message, and configures the RDNSS suppression status and interface information.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.18 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message.

ipv6 nd ra-hoplimit *value*

Use the **no** form of this command to restore the default setting.

no ipv6 nd ra-hoplimit

Parameter Description

Parameter	Description
value	The hop count in the RA message. The value range is 0-255.

Defaults The default is 64.

Command Mode Interface configuration mode

Default Level 14

Usage Guide

Configuration 1: The following example sets the hop limit to send RA message on GigabitEthernet 0/1 as 110.

Examples

```
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110
```

Verification Run the **show ipv6 interface** [*interface-id*] **ra-info** command to view the hop limit in RA message.

Prompt Messages

Common Errors

Platform Description N/A

3.19 ipv6 nd ra-interval

Use this command to set the interval of sending the RA.

ipv6 nd ra-interval { *seconds* | **min-max** *min_value max_value* }

Use the **no** form of this command to restore the default setting.

no ipv6 nd ra-interval

Parameter Description

Parameter	Description
seconds	The sending interval of RA message, in seconds. The default is 600 seconds.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds
max_value	Maximum interval sending the RA message in seconds

Defaults 600s. The actual interval of sending the RA message will be fluctuated 20% based on 600s.

Command Mode Interface configuration mode

Default Level 14

Usage Guide If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuration Examples 1: The following example sets the sending interval of RA message to be 110 seconds on Gigabit Ethernet 0/1.

```
Hostname(config-if)# ipv6 nd ra-interval 110
```

2: The following example sets the sending interval of RA message from 110 seconds to 120 seconds on Gigabit Ethernet 0/1.

```
Hostname(config-if)# ipv6 nd ra-interval min-max 110 120
```

Verification Run the **show ipv6 interface** [*interface-id*] **ra-info** command to view the sending interval of RA message on the interface.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.20 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface.

ipv6 nd ra-lifetime *seconds*

Use the **no** form of this command to restore the default setting.

no ipv6 nd ra-lifetime

Parameter Description

Parameter	Description
seconds	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

Defaults The default is 1800.

Command Mode Interface configuration mode

Default Level 14

Usage Guide The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

Configuration Examples 1: The following examples sets the lifetime of RA message on GigabitEthernet 0/1 as 2000 seconds.

```
Hostname(config-if)# ipv6 nd ra-lifetime 2000
```

Verification Run the **show ipv6 interface** [*interface-id*] **ra-info** command to view the lifetime of the router in the RA message.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.21 ipv6 nd ra-mtu

Use this command to set the MTU of the RA message.
ipv6 nd ra-mtu *value*
Use the **no** form of this command to restore the default setting.
no ipv6 nd ra-mtu

Parameter Description

Parameter	Description
value	MTU value, in the range from 0 to 4294967295. The default should be consistent with IPv6 MTU.

Defaults IPv6 MTU value of the network interface.

Command Mode Interface configuration mode

Default Level 14

Usage Guide If it is specified as 0, the RA will not have the MTU option

Configuration Examples 1: The following example sets the MTU of the RA on the interface as 1400 bytes.

```
Hostname(config -if)# ipv6 nd ra-mtu 1400
```

Verification Run the **show ipv6 interface** [*interface-id*] **ra-info** command to view MTU of the RA message.

Prompt Messages N/A

Common Errors N/A

Platform Description	N/A

3.22 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP.

ipv6 nd reachable-time *milliseconds*

Use the **no** form of this command to restore the default setting.

no ipv6 nd reachable-time

Parameter Description

Parameter	Description
milliseconds	Reachable time for the neighbor in the range from 0 to 3600000 in milliseconds.

Defaults The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

Command Mode Interface configuration mode

Default Level 14

Usage Guide The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

Configuration Examples 1: The following example sets the reachable time of the neighbor on GigabitEthernet 0/1 as 1000 seconds.

```
Hostname(config-if)# ipv6 nd reachable-time 1000000
```

Verification Run the **show ipv6 interface** command to view the reachable time in the RA message.

Prompt Messages	N/A
Common Errors	N/A
Platform Description	N/A

3.23 ipv6 nd stale-time

Use this command to set the period for the neighbor to maintain the stale state. Use the **no** form of this command to restore the default setting.

ipv6 nd stale-time *seconds*

no ipv6 nd stale-time

Parameter Description

Parameter	Description
Seconds	Sets the period for the neighbor to maintain the stale state, in the range from 0 to 86400 in seconds.

Defaults Specifies the duration for which the neighbor status is migrated to the stale state. The default is 3600.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to set the period for the neighbor to maintain the stale state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

Configuration Examples 1: The following example sets the period to 600 seconds for the neighbor to maintain the stale state.

```
Hostname(config)# ipv6 nd stale-time 600
```

Verification Run the **show running-config** command to view whether the configuration takes effect.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.24 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message.

ipv6 nd suppress-ra

Use the **no** form of this command to enable the function.

no ipv6 nd suppress-ra

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the RA message will not be sent on the IPv6 interface.

Command Mode Interface configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples 1: The following example suppresses sending RA message on GigabitEthernet 0/1.

```
Hostname(config-if)# ipv6 nd suppress-ra
```

Verification Run the **show ipv6 interface** command to view whether the RA message sending function is suppressed.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.25 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries.

ipv6 nd unresolved *number*

Use the **no** form of this command to restore the default setting.

no ipv6 nd unresolved

Parameter Description

Parameter	Description
number	Sets the maximum number of the unresolved

	neighbor table entries, in the range from 1 to 512.

Defaults The default is 0. (The maximum number is the neighbor table size supported by the device)

Command Mode Global configuration mode

Default Level 14

Usage Guide To prevent malicious scanning attacks from generating a large number of unresolved ND table entries and consuming table entry resources, you can run this command to limit the number of unresolved ND table entries.

Configuration Examples 1: The following example sets the maximum number of the unresolved neighbor table entries to 200.

```
Hostname(config)# ipv6 nd unresolved 200
```

Verification Run the **show running-config** command to view whether the configuration is consistent.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.26 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete a static neighbor.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor *ipv6-address interface-id*

Parameter Description

Parameter	Description
ipv6-address	The neighbor IPv6 address, in the form as defined in RFC4291.
interface-id	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
hardware-address	The 48-bit MAC address, a dotted triple of four-digit

	hexadecimal numbers.

Defaults No static neighbor is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.
If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the **show ipv6 neighbor static** command to display the state of the static neighbor.
Use the **clear ipv6 neighbors** command to clear all neighbors learned dynamically through NDP.

Configuration Examples 1: The following example configures a static neighbor on SVI 1.

```
Hostname(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Verification Run the **show ipv6 neighbors** command to view neighbor information.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.27 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests.

ipv6 ns-linklocal-src

Use the **no** form of this command to not mandatorily use the link local address as the source

address, but to use the link local address or the global unicast address according to RFC3484 depending on the destination IPv6 address when sending neighbor requests.

no ipv6 ns-linklocal-src

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults The local address of the link is always used as the source address to send neighbor requests.

Command Mode Global configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples 1: The following example configures the interface to not mandatory use the link local address as the source address when sending neighbor requests.

```
Hostname(config)# no ipv6 ns-linklocal-src
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.28 ipv6 redirects

Use this command to enable ICMPv6 redirection.

ipv6 redirects

Use the **no** form of this command to disable ICMPv6 redirection.

no ipv6 redirects

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults	This function is enabled by default.
Command Mode	Interface configuration mode
Default Level	14
Usage Guide	N/A
Configuration Examples	1: The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1. `Hostname(config-if-GigabitEthernet 0/1)# ipv6 redirects`

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Verification	Run the **show ipv6 interface** command to view whether ICMPv6 redirection is enabled on the interface.
Prompt Messages	N/A
Common Errors	N/A
Platform Description	N/A

3.29 ipv6 source-route

Use this command to forward the IPv6 packet with route header.

ipv6 source-route

Use the **no** form of this command to restore the default setting.

no ipv6 source-route

Parameter Description	Parameter	Description
	N/A	N/A

Defaults	The **ipv6 source-route** command is disabled by default.

Command Mode Global configuration mode.

Default Level 14

Usage Guide Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

Configuration Examples 1: The following examples configures the device to forward IPv6 packets with router header.

```
Hostname(config)# no ipv6 source-route
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.30 local-proxy-nd

Use this command to enable local ND proxy on an interface.
local-proxy-nd enable

Use the **no** form of this command to restore the default setting.
no local-proxy-nd enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, local ND proxy function is not enabled on an interface.

Command Mode Interface configuration mode

Default Level 14

Usage Guide When the access is two-layer isolation or isolation between different subnets (such as sub-VLANs), the gateway will proxy the NS requests of the downlink users and answer with its own MAC if the local ND proxy function is enabled on the gateway, so that the mutual access traffic between users can be forwarded over Layer 3 of the gateway.

Configuration Examples 1: The following examples enables local ND proxy function on VLAN1 interfaces.

```
Ruijie(config-if- VLAN 1)# local-proxy-nd enable
```

Verification Run the **show running-config** command to view the configuration.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

3.31 show ipv6 address

Use this command to display the IPv6 addresses.

show ipv6 address [*interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 address configured on the device.

```
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
Hostname#
```

The following example displays the IPv6 address configured on the GigabitEthernet 0/1.

```
Hostname#show ipv6 addr gi 0/5
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
Hostname#
```

Field	Description
Global unicast address count	Indicates the number of global unicast IPv6 addresses configured on the interface.
Tentative address count	Indicates the number of tentative addresses.
Duplicate address count	Indicates the number of duplicate addresses.
Preferred address count	Indicates the number of preferred addresses.
Deprecated address count	Indicates the number of deprecated addresses.
Preferred lifetime	Indicates the preferred lifetime.
Valid lifetime	Indicates the valid lifetime.

Platform Description N/A

3.32 show ipv6 general-prefix

Use this command to display the information of the general prefix.

show ipv6 general-prefix

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

Configuration Examples

```
The following example displays the information of the general prefix.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
```

Related Commands	Command	Description
	ipv6 general-prefix	Configures the general prefix.

Platform Description N/A

3.33 show ipv6 interface

Use this command to display the IPv6 interface information.

show ipv6 interface [[[*interface-id*] [**ra-info**]] | [brief [*interface-id*]]]

Parameter Description	Parameter	Description
	interface-id	Interface (including Ethernet interface, aggregate port, or SVI)
	ra-info	Displays the RA information of the interface.
	brief	Displays the brief information of the interface (interface status and address information).

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

Configuration Examples The following example displays the information of the IPv6 interface.

```
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
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
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 device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicates that the address is an anycast address.
TENTATIVE	Indicates that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicates that a duplicate address exists.
DEPRECATED	Indicates that the preferred lifetime of the address expires.
NODAD	Indicates that no DAD is implemented for the address.
AUTOIFID	Indicates that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.
PRE	Indicates a automatically configured stateless address.

GEN	Indicates the address generated by the generic prefix.

The following example displays the RA information of the IPv6 interface. 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 device advertisements live for 1800 seconds
ND device 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)
```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning

total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
Hostname#show ipv6 interface brief

GigabitEthernet 0/1          [down/down]
       2222::2
       FE80::1614:4BFF:FE5C:ED3A
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.34 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

show ipv6 neighbors [[**verbose**] [*interface-id*] [*ipv6-address*] | [**static**]]

Parameter Description

Parameter	Description
verbose	Displays the neighbor details.
static	Displays the validity status of static neighbors.
interface-id	Displays the neighbors of the specified interface.
ipv6-addres	Displays the neighbors of the specified IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the neighbors on the SVI 1 interface:

```
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 shows the neighbor details:

```
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
```

Field	Description
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device

	/H: The neighbor is a host.
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

The following example shows the static neighbor status

```
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
```

Field	Description
IPv6 Address	Indicates the IPv6 address of a static neighbor.
Linklayer Addr	Indicates the configured link address, which is an MAC address.
Interface	Indicates the interface on which the neighbor resides.
State	Indicates the status of the static neighbor: The value of STATE can be one of the following: ACTIVE – indicates the neighbor is active. INACTIVE – indicates the neighbor is inactive. When the configured static neighbor IPV6 address does not match the address configured on the interface (that is, the configured static neighbor IPV6 address is not in the network segment of any interface address, or conflicts with the interface address), the static neighbor is inactive, that is, the data packet will not be forwarded according to the MAC address designated by the static neighbor.

Related Commands

Command	Description
ipv6 neighbor	Configures a neighbor.

Platform Description N/A

3.35 show ipv6 neighbors statistics

Use the following command to show the statistics of IPv6 neighbors.

show ipv6 neighbors statistics

Parameter

Parameter	Description

Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the statistics of the global neighbors.

```
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
Hostname#
```

Field	Description
Memory	Memory usage
Entries	Number of neighbor entries
Static	Number of static entries
Dynamic	Number of dynamic entries
Local	Number of entries corresponding to local IPv6 address
Incomplete	Number of unresolved entries
Reachable	Number of reachable entries
Stale	Number of stale entries
Delay	Number of delay entries
Probe	Number of probe entries

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.36 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

show ipv6 packet statistics [**total** | *interface-name*]

Parameter Description

Parameter	Description
total	Displays total statistics of all interfaces.
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the total statistics of the IPv6 packets and the statistics of each inerface.

```
 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
Hostname#
```

The following example displays the total statistics of the IPv6 packets.

```
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
Hostname#
```

Platform Description	N/A

3.37 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

show ipv6 raw-socket [*num*]

Parameter Description	**Parameter**	**Description**
	num	Protocol.

Defaults	N/A
Command Mode	Privileged EXEC mode.
Usage Guide	N/A

Configuration Examples The following example displays all IPv6 raw sockets.

```
Hostname# show ipv6 raw-socket
Number Protocol Process name
1      ICMPv6   vrrp.elf
2      ICMPv6   tcpip.elf
3      VRRP     vrrp.elf
Total: 3
```

Field	**Description**
Number	Number.
Protocol	Protocol.
Process name	Process number.
Total	Total number of IPv6 raw sockets.

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

3.38 show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.

show ipv6 routers [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Displays the routing advertisement of the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

Configuration Examples The following example displays the IPv6 router

```
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 seconds, preferred lifetime 604800 seconds
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.39 show ipv6 sockets

Use this command to display all IPv6 sockets.

show ipv6 sockets

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 sockets.

```
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
```

Field	Description
Number	Number.
Process name	Process name.
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.
Protocol	Protocol number
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	State (for IPv6 TCP sockets).
Total	Total number of sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.40 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

show ipv6 udp [**local-port** *num*] [**peer-port** *num*]

Use this command to display IPv6 UDP socket statistics.

show ipv6 udp statistics

Parameter Description

Parameter	Description
local-port *num*	Local port number.
peer-port *num*	Peer port number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all IPv6 UDP sockets.

```
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
```

Filed	Description
Number	Number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4 DHCP Commands

4.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the **no** form of this command to restore the default setting.

address range *low-ip-address high-ip-address*

no address range

Parameter Description

Parameter	Description
low-ip-address	Start address in the network segment range.
high-ip-address	End address in the network segment range.

Defaults By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.

Command Mode Address pool CLASS configuration mode.

Usage Guide Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple classes. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

Configuration Examples The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```
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
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
class	Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode.

Platform Description N/A

4.2 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

bootfile *file-name*

no bootfile

default bootfile

Parameter Description

Parameter	Description
file-name	Startup file name.

Defaults No startup file name is defined by default.

Command Mode DHCP address pool configuration mode

Usage Guide Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

Configuration Examples The following example enables DHCP server and relay feature.

```
Hostname(dhcp-config)# bootfile router.conf
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
next-server	Configures the next server IP address of the DHCP client startup process.

Platform Description N/A

4.3 class

Use this command to configure the associated CLASS in the DHCP address pool. Use the **no** form of this command to restore the default setting.

class *class-name*

no class

Parameter Description

Parameter	Description
class-name	Class name, which can be the character string or numeric such as myclass or 1.

Defaults By default, no CLASS is associated with the address pool.

Command Mode DHCP address pool configuration mode

Usage Guide Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSes, and each CLASS can specify different network segment range.

During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSes in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSes are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same as the range of address pool where the CLASS is.

Configuration Examples The following example configures the address *mypool0* to associate with class1.

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# class class1
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.4 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode.

clear ip dhcp binding { * | *ip-address* }

Parameter Description

Parameter	Description
*	Deletes all DHCP bindings.
ip-address	Deletes the binding of the specified IP addresses.

Defaults N/A.

Command Privileged EXEC mode.

Mode

Usage Guide This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

Configuration Examples The following example clears the DHCP binding with the IP address 192.168.12.100.

```
Hostname# clear ip dhcp binding 192.168.12.100
```

Related Commands

Command	Description
show ip dhcp binding	Displays the address binding of the DHCP server.

Platform Description N/A

4.5 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

clear ip dhcp conflict { * | *ip-address* }

Parameter Description

Parameter	Description
*	Deletes all DHCP address conflict records.
ip-address	Deletes the conflict record of the specified IP addresses.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** command can be used to delete the history conflict record.

Configuration Examples The following example clears all address conflict records.

```
Hostname# clear ip dhcp conflict *
```

Related Commands

Command	Description
ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Displays the address conflict that the DHCP server detects when it assigns an IP address.

Platform N/A

Description

4.6 clear ip dhcp history

Use this command to clear the address assigned by the DHCP server.

clear ip dhcp history{ * | *mac-address* }

Parameter Description	**Parameter**	**Description**
	*	Clears all addresses assigned by the DHCP server.
	mac-address	Clears the address assigned by the DHCP server corresponding to the specified MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is configured on the DHCP server.

Configuration Examples The following example clears all addresses assigned by the DHCP server.

```
Hostname# clear ip dhcp history *
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.7 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.

clear ip dhcp relay statistics

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The DHCP relay is configured with the counter to count various packets received or transmitted by the relay. This command is used to clear the counters.

Configuration Examples The following example clears the DHCP relay statistics.

```
Hostname# clear ip dhcp relay statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 clear ip dhcp server rate

Use this command to clear statistics about the packet processing rate of every module.

clear ip dhcp server rate

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.

Configuration Examples The following example clears statistics about the packet processing rate of every module.

```
Hostname# clear ip dhcp server rate
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

clear ip dhcp server statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.

Configuration Examples The following example clears the statistics record of the DHCP server.

```
Hostname# clear ip dhcp server statistics
```

Related Commands

Command	Description
show ip dhcp server statistics	Displays the statistics record of the DHCP server.

Platform Description N/A

4.10 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

client-identifier *unique-identifier*

no client-identifier

Parameter Description

Parameter	Description
unique-identifier	The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

Defaults N/A.

Command Mode DHCP address pool configuration mode.

Usage Guide When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media.

The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700.

This command is used only when the DHCP is defined by manual binding.

Configuration Examples The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
Hostname#(dhcp-config)#                                    client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

Related Commands

Command	Description
hardware-address	Defines the hardware address of DHCP client.
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.11 client-name

Use this command to define the name of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

client-name *client-name*

no client-name

Parameter Description

Parameter	Description
client-name	Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

Defaults No client name is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.

Configuration Examples The following example defines a string river as the name of the client.

```
Hostname(dhcp-config)# client-name river
```

Related Commands

Command	Description
host	Defines the IP address and network mask, which is used to

	configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.12 default-router

Use this command to define the default gateway of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

default-router *ip-address* [*ip-address2…ip-address8*]

no default-router

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the equipment. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 gateways can be configured.

Defaults No gateway is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

Configuration Examples The following example defines 192.168.12.1 as the default gateway.

```
Hostname(dhcp-config)# default-router 192.168.12.1
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.13 dns-server

Use this command to define the DNS server of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

dns-server { *ip-address* [*ip-address2…ip-address8*] }

default dns-server
no dns-server

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the DNS server. At least one IP address should be configured.
ip-address2…ip-address8	(Optional) Up to 8 DNS servers can be configured.

Defaults No DNS server is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one DNS server is defined, the former will possess higher priory, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails.

Configuration Examples The following example specifies the DNS server 192.168.12.3 for the DHCP client.

```
Hostname(dhcp-config)# dns-server 192.168.12.3
```

Related Commands

Command	Description
domain-name	Defines the suffix domain name of the DHCP client.
ip address dhcp	Enables the DHCP client on the interface to obtain the IP address information.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.14 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.
domain-name *domain-name*
no domain-name

Parameter Description

Parameter	Description
domain-name	Defines the suffix domain name string of the DHCP client.

Defaults No suffix domain name by default.

Command Mode DHCP address pool configuration mode.

Usage Guide After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

Configuration Examples The following example defines the suffix domain name i-net.com.cn for the DHCP client.

```
Hostname(dhcp-config)#domain-name test.com.cn
```

Related Commands

Command	Description
dns-server	Defines the DNS server of the DHCP client.
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.

Platform Description N/A

4.15 hardware-address

Use this command to define the hardware address of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

hardware-address *hardware-address* [*type*]

no hardware-address

Parameter Description

Parameter	Description
hardware-address	Define the MAC address of the DHCP client.
type	To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition. String option: Ethernet ieee802 Digits option: 1 (10M Ethernet) 6 (IEEE 802)

Defaults No hardware address is defined by default.

If there is no option when the hardware address is defined, it is the Ethernet by default.

Command Mode DHCP address pool configuration mode.

Usage Guide This command can be used only when the DHCP is defined by manual binding.

Configuration Examples The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
Hostname(dhcp-config)# hardware-address 00d0.f838.bf3d
```

Related Commands

Command	Description
client-identifier	Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
default-router	Defines the default route of the DHCP client.

Platform Description N/A

4.16 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

host *ip-address* [*netmask*]

no host

Parameter Description

Parameter	Description
ip-address	Defines the IP address of DHCP client.
netmask	Defines the network mask of DHCP client.

Defaults No IP address or network mask of the host is defined.

Command Mode DHCP address pool configuration mode.

Usage Guide If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

Configuration Examples The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
Hostname(dhcp-config)# host 192.168.12.91 255.255.255.240
```

Related Commands

Command	Description
client-identifier	Defines the unique ID of the DHCP client (Indicated in hex and separated by dot).
hardware-address	Defines the hardware address of DHCP client.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

default-router	Define the default route of the DHCP client.	**default-router**

Platform Description N/A

4.17 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip address dhcp

no ip address dhcp

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults The interface cannot obtain the ID address by the DHCP by default.

Command Mode Interface configuration mode.

Usage Guide When requesting the IP address, the DHCP client of the system software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional).

The client of the system software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.

Configuration Examples The following example makes the FastEthernet 0 port obtain the IP address automatically.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1) ip address dhcp
```

Related Commands	**Command**	**Description**
	dns-server	Defines the DNS server of DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.18 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp class *class-name*

no ip dhcp class *class-name*

Parameter Description

Parameter	Description
class-name	Class name, which can be character string or numeric such as myclass or 1.

Defaults By default, the class is not configured.

Command Mode Global configuration mode.

Usage Guide After executing this command, it enters the global CLASS configuration mode which is shown as "Hostname(config-dhcp-class)#". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

Configuration Examples The following example configures a global CLASS.

```
Hostname(config)# ip dhcp class myclass
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.19 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

Parameter Description

Parameter	Description
low-ip-address	Excludes the IP address, or excludes the start IP address within the range of the IP address.
high-ip-address	Excludes the end IP address within the range of the IP address.

Defaults The DHCP server assigns the IP addresses of the whole address pool by default.

Command Mode Global configuration mode.

Usage Guide If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

Configuration Examples The following example sets the DHCP server to not attempt to assign the IP addresses within 192.168.12.100~150.

```
Hostname(config)#ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

The following example deletes the excluded address range in Example 1.

```
Hostname(config)#no ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

4.20 ip dhcp force-send-nak

Use this command to configure the forcible NAK packet sending function. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp force-send-nak

no ip dhcp force-send-nak

default ip dhcp force-send-nak

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending

DHCPDISCOVER packets. The forcible NAK packet sending function is added to shorten the interval at which the client sends DHCPDISCOVER packets.

Configuration Examples The following example enables the forcible NAK packet sending function in global configuration mode.

```
Hostname(config)# ip dhcp force-send-nak
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.21 ip dhcp monitor-vrrp-state

Use this command in layer-3 configuration mode to enable the DHCP Server to monitor the status of VRRP interfaces so that the DHCP Server processes only those packets sent from a VRRP interface in the Master state. Use the **no** form of this command to restore the default setting. If it is canceled, the DHCP Server processes packets from VRRP interfaces in the Master or Backup state.

ip dhcp monitor-vrrp-state

no ip dhcp monitor-vrrp-state

Parameter Description

Parameter	Description
N/A	N/A

Defaults The **ip dhcp monitor-vrrp-state** command is disabled by default. .

Command Mode Layer-3 interface configuration mode.

Usage Guide If a VRRP address is configured for an interface, the DHCP Server processes packets sent from the master interface and discards packets sent from the backup interface. If no VRRP address is configured, the DHCP Server does not monitor the status of VRRP interfaces. All DHCP packets will be processed.

Configuration Examples The following example enables the DHCP Server to monitor the status of VRRP interfaces.

```
Hostname(config-if)# ip dhcp monitor-vrrp-state
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.22 ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp ping packets [*number*]

no ip dhcp ping packets

Parameter Description

Parameter	Description
number	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

Defaults The Ping operation sends two packets by default.

Command Mode Global configuration mode.

Usage Guide When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.

Configuration Examples The following example sets the number of the packets sent by the ping operation as 3.

```
Hostname(config)# ip dhcp ping packets 3
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears the DHCP history conflict record.
ip dhcp ping packet	Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
show ip dhcp conflict	Displays the DHCP server detects address conflict when it assigns an IP address.

Platform Description N/A

4.23 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

Parameter Description

Parameter	Description
milli-seconds	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Defaults The default is 500 seconds.

Command Mode Global configuration mode.

Usage Guide This command defines the time that the DHCP server waits for a ping response packet.

Configuration Examples The following example configures the waiting time of the ping response packet to 600ms.

```
Hostname(config)#ip dhcp ping timeout 600
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears the DHCP history conflict record.
ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Displays the address conflict the DHCP server detects when it assigns an IP address.

Platform Description N/A

4.24 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

Parameter Description

Parameter	Description
pool-name	A string of characters and positive integers, for instance, mypool or 1.

Defaults No DHCP address pool is defined by default.

Command Mode Global configuration mode.

Usage Guide Execute the command to enter the DHCP address pool configuration mode:

```
Hostname(dhcp-config)#
```

In this configuration mode, configure the IP address range, the DNS server and the default gateway.

Configuration Examples The following example defines a DHCP address pool named mypool0.

```
Hostname(config)#ip dhcp pool mypool0
Hostname(dhcp-config)#
```

Related Commands

Command	Description
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

4.25 ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check** *server-id* function. Use the **no** form of this command to restore the default setting.

ip dhcp relay check server-id

no ip dhcp relay check server-id

Parameter Description

Parameter	Description
N/A	N/A

Defaults The **ip dhcp relay check server-id** command is disabled.

Command Mode Global configuration mode.

Usage Guide Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

Configuration Examples The following example enables the ip dhcp relay check server-id function.

```
Hostname(config)# ip dhcp relay check server-id
```

Related

Command	Description

Commands	service dhcp	Enables the DHCP Relay.

Platform Description N/A

4.26 ip dhcp relay information circuit-id format

Use this command to set the custom string for circuit-id. Use the **no** form of this command to restore the default setting.

ip dhcp relay information circuit-id format {hex | ascii} [*string*]

no ip dhcp relay information circuit-id format {hex | ascii}

Parameter Description

Parameter	Description
hex	Hexadecimal
ascii	ASCII code.
string	Custom string

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay information circuit-id format** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the custom string for circuit-id.

```
Hostname(config)# ip dhcp relay information circuit-id format hex abc111
Hostname(config)# ip dhcp relay information circuit-id format ascii device-test
```

The following example disables this function.

```
Hostname(config)# no ip dhcp relay information circuit-id format hex
Hostname(config)# no ip dhcp relay information circuit-id format ascii
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.27 ip dhcp relay information circuit-id string

Use this command to set the device name for circuit-id. Use the **no** form of this command to restore the default setting.

ip dhcp relay information circuit-id string [*devicename*]

no ip dhcp relay information option82

Parameter Description

Parameter	Description
devicename	Sets the device name.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay information circuit-id string** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the device name for circuit-id.

```
Hostname(config)# ip dhcp relay information circuit-id string device-name
```

The following example disables this function.

```
Hostname(config)# no ip dhcp relay information circuit-id string
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.28 ip dhcp relay information option82

Use this command to enable the **ip dhcp relay information option82** function. Use the **no** form of this command to restore the default setting.

ip dhcp relay information option82

no ip dhcp relay information option82

Parameter Description

Parameter	Description
N/A	N/A

Defaults The **ip dhcp relay information option82** command is disabled.

Command Global configuration mode.

Mode

Usage Guide This command is exclusive with the **option dot1x** command.

Configuration Examples The following example enables the option82 function on the DHCP relay.

```
Hostname# configure terminal
Hostname(config)# Ip dhcp relay information option82
```

Related Commands

Command	Description
service dhcp	Enables the DHCP Relay.

Platform Description N/A

4.29 ip dhcp relay information remote-id format

Use this command to set the custom string for remote-id.. Use the **no** form of this command to restore the default setting.

ip dhcp relay information remote-id format { **hex | ascii** } [*string*]

no ip dhcp relay information remote-id format { **hex | ascii** }

Parameter Description

Parameter	Description
hex	Hexadecimal
ascii	ASCII code
string	Custom string

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay information remote-id format** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the custom string for circuit-id.

```
Hostname(config)# ip dhcp relay information remote-id format hex abc111
Hostname(config)# ip dhcp relay information remote-id format ascii port-test
```

The following example disables this function.

```
Hostname(config)# no ip dhcp relay information remote-id format hex
Hostname(config)# no ip dhcp relay information remote-id format ascii
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.30 ip dhcp relay information remote-id string

Use this command to set the port name for remote-id. Use the **no** form of this command to restore the default setting.

ip dhcp relay information remote-id string [*portname*]

no ip dhcp relay information remote-id string

Parameter Description	Parameter	Description
	portname	Sets the port name.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay information remote-id string** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the port name for remote-id.

```
Hostname(config)# ip dhcp relay information remote-id string port-name
```

The following example disables this function.

```
Hostname(config)# no ip dhcp relay information remote-id string
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.31 ip dhcp relay-information remote-id format

Use this command to set the custom string for remote-id on an interface. Use the **no** form of this command to restore the default setting.

ip dhcp relay-information remote-id format {hex | ascii} [*string*]

no ip dhcp relay-information remote-id format {hex | ascii}

Parameter Description

Parameter	Description
hex	Hexadecimal
ascii	ASCII code
string	Custom string

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay-information remote-id format** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the custom string for circuit-id.

```
Hostname(config-if-GigabitEthernet 0/2)# ip dhcp relay information remote-id format hex abc111
Hostname(config-if-GigabitEthernet 0/2)# ip dhcp relay information remote-id format ascii port-test
```

The following example disables this function.

```
Hostname(config-if-GigabitEthernet 0/2)# no ip dhcp relay information remote-id format hex
Hostname(config-if-GigabitEthernet 0/2)# no ip dhcp relay information remote-id format ascii
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.32 ip dhcp relay-information remote-id string

Use this command to set the port name for remote-id on an interface. Use the **no** form of this command to restore the default setting.

ip dhcp relay-information remote-id string [*portname*]

no ip dhcp relay-information remote-id string

Parameter Description

Parameter	Description
portname	Sets the port name.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is configured on the DHCP Relay. When you configure the **ip dhcp relay-information remote-id string** command, the device, as the DHCP Relay, adds the option information in the DHCP request packets.

Configuration Examples The following example sets the port name for remote-id on an interface.

```
Hostname(config-if-GigabitEthernet 0/2)# ip dhcp relay-information remote-id string if-port-name
```

The following example disables this function.

```
Hostname(config-if-GigabitEthernet 0/2)# no ip dhcp relay-information remote-id string
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.33 ip dhcp server arp-detect

Use this command to enable the user-offline detection. Use the **no** or **default** form this command to restore the default setting.

ip dhcp server arp-detect

no ip dhcp server arp-detect

default ip dhcp server arp-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to detect whether the user has gone offline, If the user does not go online within a certain period, the IP address is reclaimed.

Configuration Examples The following example enables the user-offline detection.

```
Hostname(config)# ip dhcp server arp-detect
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

4.34 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the **no** form of this command can be used to disable the CLASS.

ip dhcp use class

no ip dhcp use class

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults Enabled

Command Mode This function is enabled by defualt.

Usage Guide N/A

Configuration Examples The following example enables the CLASS to allocate addresses.

```
Hostname(config)# ip dhcp use class
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.35 ip helper-address

Use this command to add an IP address of the DHCP server. Use the **no** form of this command to delete an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

ip helper-address { cycle-mode | *A.B.C.D* **}**

no ip helper-address { cycle-mode | *A.B.C.D* **}**

Parameter Description	**Parameter**	**Description**
	cycle-mode	Forwards the DHCP request packets to all DHCP servers.

A.B.C.D	DHCP server IP address

Defaults N/A

Command Mode Global configuration mode, interface configuration mode.

Usage Guide Up to 20 DHCP server IP addresses can be configured globally or on a layer-3 interface.
One DHCP request of this interface will be sent to these servers. You can select one for confirmation.

Configuration Examples The following example configures IP address 192.168.11.1 for the DHCP server on interface vlan 1.

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# interface vlan 1
Hostname(config-if)# ip helper-address 192.168.11.1
```

The following example deletes IP address 192.168.11.1 for the DHCP server on interface vlan 1.

```
Hostname(config-if)# no ip helper-address 192.168.11.1
```

The following example configures the IP address 192.168.11.1 for the DHCP server globally.

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# ip helper-address 192.168.100.1
```

The following example deletes the IP address 192.168.11.1 for the DHCP server globally.

```
Hostname(config)# no ip helper-address 192.168.100.1
```

The following example enables DHCP request to be forwarded by all DHCP servers.

```
Hostname(config)# ip helper-address cycle-mode
```

The following example disables DHCP request to be forwarded by all DHCP servers.

```
Hostname(config)# no ip helper-address cycle-mode
```

Related Commands

Command	Description
service dhcp	Enables the DHCP relay.

Platform Description N/A

4.36 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

Parameter

Parameter	Description

Description

days	Lease time in days
hours	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
minutes	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
infinite	Infinite lease time.

Defaults The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.

Command Mode DHCP address pool configuration mode.

Usage Guide When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

Configuration Examples The following example sets the DHCP lease to 1 hour.

```
Hostname(dhcp-config)# lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
Hostname(dhcp-config)# lease 0 0 1
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.37 lease-threshold

Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold. Use the **default** or **no** form of this command to restore the default setting.

lease-threshold *percentage*

default lease-threshold

no lease-threshold

Parameter Description

Parameter	Description
percentage	Usage of the address pool, ranging from 60 to 100 in percentage.

Defaults 90

Command Mode DHCP address pool configuration mode.

Usage Guide If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.

Configuration Examples The following example sets the alarm threshold to 80%.

```
Hostname(dhcp-config)# lease-threshold 80
```

The following example disables the address pool alarm function.

```
Hostname(dhcp-config)# no lease-threshold
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.38 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** form of this command can be used to restore the default setting.

netbios-name-server *ip-address* [*ip-address2…ip-address8*]

netbios-name-server

Parameter Description

Parameter	Description
ip-address	IP address of the WINS server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

Defaults No WINS server is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one WINS server is defined, the former has higher priory. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

Configuration Examples The following example specifies the WINS server 192.168.12.3 for the DHCP client.

```
Hostname(dhcp-config)# netbios-name-server 192.168.12.3
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client on the interface to obtain the IP address.
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
netbios-node-type	Defines the netbios node type of the client host.

Platform Description N/A

4.39 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the **no** form of this command to restore the default setting.

netbios-node-type *type*

no netbios-node-type

Parameter Description

Parameter	Description
type	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node m-node: mixed node h-node: hybrid node

Defaults No type of the NetBIOS node is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.

By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is

not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

Configuration Examples The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
Hostname(dhcp-config)# netbios-node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

Platform Description N/A

4.40 network

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

network *net-number net-mask*

no network

Parameter Description

Parameter	Description
net-number	Network number of the DHCP address pool
net-mask	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.

Defaults No network number or network mask is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

Configuration The following example defines the network number of the DHCP address pool as 192.168.12.0, and

Examples the network mask as 255.255.255.240.

```
Hostname(dhcp-config)# network 192.168.12.0 255.255.255.240
```

Related Commands

Command	Description
ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.41 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the **no** form of this command to restore the default setting.

next-server *ip-address* [*ip-address2…ip-address8*]

no next-server

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 startup servers can be configured.

Defaults N/A

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.

Configuration Examples The following example specifies the startup server 192.168.12.4 for the DHCP client.

```
Hostname(dhcp-config)# next-server 192.168.12.4
```

Related Commands

Command	Description
bootfile	Defines the default startup mapping file name of the DHCP client.
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
ip help-address	Defines the Helper address on the interface.
option	Configures the option of the system software DHCP server.

Platform N/A

Description

4.42 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no option

Parameter Description

Parameter	Description
code	Defines the DHCP option codes.
ascii *string*	Defines an ASCII string.
hex *string*	Defines a hex string.
ip *ip-address*	Defines an IP address list.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

Configuration Examples The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
Hostname(dhcp-config)# option 19 hex 1
```

The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
Hostname(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0
192.168.12.16
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.43 pool-status

Use this command to enable or disable the DHCP address pool.

pool-status { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the address pool.
disable	Disables the address pool.

Defaults By default, the address pool is enabled after it is configured.

Command Mode DHCP address pool configuration mode

Usage Guide This command is configured on the DHCP server.

Configuration Examples The following example disables the address pool.

```
Hostname(dhcp-config)# pool-status disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.44 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the **no** form of this command to delete the Option82 matching information of the CLASS.

relay agent information

no relay agent information

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Global CLASS configuration mode

Mode

Usage Guide After executing this command, it enters the Option82 matching information configuration mode which is shown as “Hostname(config-dhcp-class-relayinfo)#”.
In this configuration mode, user can configure the class matching multiple Option82 information.

Configuration Examples The following example configures a global CLASS and enters the Option82 matching information configuration mode.

```
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# relay agent information
Hostname(config-dhcp-class-relayinfo)#
```

Related Commands

Command	Description
ip dhcp class	Defines a CLASS and enters the global CLASS configuration mode.

Platform Description N/A

4.45 relay-information hex

Use this command to enter the Option82 matching information configuration mode. Use the **no** form of this command to delete a piece of matching information.
relay-information hex *aabb.ccdd.eeff…* [*]
no relay-information hex *aabb.ccdd.eeff…* [*]

Parameter Description

Parameter	Description
aabb.ccdd.eeff…[*]	Hexadecimal Option82 matching information. The ‘*’ symbol means partial matching which needs the front part matching only. Without the ‘*’ means needing full matching.

Defaults N/A

Command Mode Global CLASS configuration mode

Usage Guide N/A

Configuration Examples The following example configures a global CLASS which can match multiple Option82 information.

```
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*
```

Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.
	relay agent information	Enters the Option82 matching information configuration mode.

Platform Description N/A

4.46 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the **no** form of this command to delete the identification.

remark *class-remark*

no remark

Parameter Description	Parameter	Description
	class-remark	Information used to identify the CLASS, which can be the character strings with space in them.

Defaults N/A.

Command Mode Global CLASS configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the identification information for a global CLASS.

```
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# remark used in #1 build
```

Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.

Platform Description N/A

4.47 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global

configuration mode. Use the **no** form of this command to restore the default setting.

service dhcp

no service dhcp

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults The **service dhcp** command is disabled.

Command Mode Global configuration mode

Usage Guide The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.

Configuration Examples The following example enables the DHCP server and the DHCP relay feature.

```
Hostname(config)# service dhcp
```

Related Commands	**Command**	**Description**
	show ip dhcp server statistics	Displays various statistics information of the DHCP server.
	ip helper-address [**vrf**] *A.B.C.D*	Adds an IP address of the DHCP server.

Platform Description N/A

4.48 show dhcp lease

Use this command to display the lease information of the IP address obtained by the DHCP client.

show dhcp lease

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide If the IP address is not defined, display the binding condition of all addresses. If the IP address is defined, display the binding condition of this IP address.

Configuration Examples The following example displays the result of the show dhcp lease.

```
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: 3 Bound
 DHCP transaction id: 168F
 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: redgaint-00d0.f8fb.5740-Fa0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.49 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

show ip dhcp binding [*ip-address*]

Parameter Description

Parameter	Description
ip-address	(Optional) Only displays the binding condition of the specified IP addresses.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address

Configuration Examples The following is the result of the show ip dhcp binding.

```
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
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.
Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

Related Commands

Command	Description
clear ip dhcp binding	Clears the DHCP address binding table.

Platform Description N/A

4.50 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

show ip dhcp conflict

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command can display the conflict address list detected by the DHCP server.

Configuration Examples The following example displays the output result of the **show ip dhcp conflict** command.

```
Hostname# show ip dhcp conflict
IP address  Detection Method
 192.168.12.1  Ping
```

The meaning of various fields in the show result is described as follows.

Field	Description

IP address	The IP addresses which cannot be assigned to the DHCP client.
Detection Method	The conflict detection method.

Related Commands

Command	Description
clear ip dhcp conflict	Clears the DHCP conflict record.

Platform Description N/A

4.51 show ip dhcp identifier

Use this command to display the DHCP address pool ID and address usage.

show ip dhcp identifier

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the DHCP address pool ID and address usage.

```
Hostname# show ip dhcp identifier
Pool  name    Identifier     Total    Distributed  Remained
------------  -----------  -----------  -----------  --------
wwp           597455782    65533        0            65533
```

Pool name	Address pool name.
Identifier	Address pool ID.
Total	Total number of addresses.
Distributed	Number of allocated addresses.
Remained	Number of remained addresses.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.52 show ip dhcp pool

Use this command to display the address statistics of an address pool.

show ip dhcp pool [*poolname*]

Parameter Description	Parameter	Description
	poolname	(Optional) Address pool whose address statistics are to be displayed.

Defaults Privileged EXEC mode.

Command Mode N/A

Usage Guide Use this command to show the address statistics of an address pool.

Configuration Examples The following example displays the output result of the **show ip dhcp pool** *poolname* command.

```
Hostname# show ip dhcp poolname
Pool poolname:
 Address range    192.168.0.1 - 192.168.0.254
 Class range     192.168.0.1 - 192.168.0.254
 Total address    252
Excluded     2
Distributed    30
Conflict     10
Remained     212
Usage percentage    84.12698%
Lease threshold    90%
```

The meaning of various fields in the show result is described as follows.

Field	Description
Address range	Address range of the address pool.
Class range	Class address range. By default, the address range for the same address pool is not configured. Otherwise, the class range is displayed.
Total address	Total number of addresses that can be assigned in the address pool.
Excluded	Number of excluded addresses.
Distributed	Number of assigned addresses.
Conflict	Number of conflicting addresses in the address pool.
Remained	Number of remaining addresses that have not been assigned or can be reused.
Usage percentage	Address pool usage.
Lease threshold	Lease threshold.

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform Description N/A

4.53 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

show ip dhcp relay-statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the statistics of the DHCP relay.

Configuration Examples The following example displays the statistics of the DHCP relay.

```
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
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.54 show ip dhcp server statistics

Use this command to display the statistics of the DHCP server.

show ip dhcp server statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the statistics of the DHCP server.

Configuration Examples The following example displays the output result of the **show ip dhcp server statistics** command.

```
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
DHCPREQTIMES           0
DHCPREQSUCTIMES        0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE       0
NO-LEASE-RESOURCE      0
SERVERID-NO-MATCH       0
-----------------------------------------
recv                      0
send                      0
```

The meaning of various fields in the show result is described as follows.

Field	Description
Address pools	Number of address pools.
Lease count	Number of allocated lease.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.

Related Commands

Command	Description
clear ip dhcp server statistics	Clears the DHCP server statistics.

Platform Description N/A

4.55 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

show ip dhcp socket

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the socket used by the DHCP server.

```
Hosname#show ip dhcp socket
dhcp socket = 47.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5 DNS Commands

5.1 clear host

Use this command to clear the dynamically learned host name.

clear host [* | *host-name*]

Parameter Description

Parameter	Description
host-name	Deletes the specified dynamic domain name buffer.
*	Deletes all dynamic domain name buffer.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

Configuration Examples The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.

```
Hostname(config)#clear host *
```

Related Commands

Command	Description
show hosts	Displays the host name buffer table.

Platform Description N/A

5.2 ip domain-lookup

Use this command to enable DNS domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide This command enables the domain name resolution function.

Configuration Examples The following example disables the DNS domain name resolution function.

```
Hostname(config)# no ip domain-lookup
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

5.3 ip host

Use this command to configure the mapping of the host name and the IP address. Use the **no** form of the command to remove the host list.

ip host *host-name ip-address*

no ip host *host*-name *ip-address*

Parameter Description

Parameter	Description
host-name	The host name of the equipment
telnet-port	Port number for telnet. The value is from 0 to 65535. The default value is 0.
ip-address	The IP address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures IPv4 address 192.168.5.243 for domain name www .test.com.

```
Hostname(config)# ip host www.test.com 192.168.5.243
```

Related Commands

Command	Description
show hosts	Show the DNS related configuration information.

Platform Description N/A

5.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server { *ip-address* | *ipv6-address }*

no ip name-server [*ip-address* | *ipv6-address*]

Parameter Description

Parameter	Description
ip-address	The IP address of the domain name server.
ipv6-address	The IPv6 address of the domain name server.

Defaults No domain name server is configured by default.

Command Mode Global configuration mode.

Usage Guide Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.

Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

Configuration Examples N/A

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

5.5 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

ipv6 host *host-name* [*telnet-port*] *ipv6-address*

no ipv6 host *host*-name [*telnet-port*] *ipv6-address*

Parameter Description

Parameter	Description
host-name	The host name of the equipment
telnet-port	Port number for telnet. The value is from 0 to 65535. The default value is 0.
ipv6-address	The IPv6 address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide To delete the host list, use the **no ipv6 host** *host-name ipv6-address* command.

Configuration Examples The following example configures the IPv6 address for the domain name.

```
Hostname(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

5.6 show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Parameter Description

Parameter	Description
hostname	Displays the specified domain name information,

Defaults All domain name information is displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide This command is used to display the DNS related configuration information.

Configuration Examples

```
Hostname# show hosts
Name servers are:
192.168.5.134 static

Host             type         Address             TTL(sec)
switch           static       192.168.5.243          ---
www.test.com   dynamic     192.168.5.123          126
```

Field	Description
Name servers	Domain name server
Host	Domain name
type	Resolution type: Static resolution and dynamic resolution.
Address	IP address corresponding to the domain name
TTL	TTL of entries corresponding to the domain name/IP address.

Related Commands

Command	Description
ip host	Configures the host name and IP address mapping by manual.
ipv6 host	Configures the host name and IPv6 address mapping by manual.
ip name-server	Configures the DNS server.

Platform Description N/A

6 FTP Server Commands

6.1 ftp-server enable

Use this command to enable the FTP server. Use the **default** form of this command to restore the default setting.

ftp-server enable

default ftp-server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the FTP server to connect the FTP client to upload/download the files.

Configuration Examples The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory:

```
Hostname(config)# ftp-server topdir /syslog
Hostname(config)# ftp-server enable
```

The following example disables the FTP Server:

```
Hostname(config)# no ftp-server enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.2 ftp-server login timeout

Use this command to set the timeout interval for login to the FTP server. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login timeout *time*

no ftp-server login timeout

default ftp-server login timeout

Parameter Description

Parameter	Description
time	Sets the timeout interval for login to the FTP server, in the range from 1 to 30 in the unit of minutes.

Defaults The default is 2 minutes.

Command Mode Global configuration mode

Usage Guide The timeout interval refers to the maximum time when your account is allowed online after you login to the server. If you don't perform authentication again before the timeout interval expires, you will be forced offline.

Configuration Examples The following example sets the timeout interval for login to the FTP server to 5 minutes.

```
Hostname(config)# ftp-server login timeout 5
```

The following example restores the default setting.

```
Hostname(config)# no ftp-server login timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.3 ftp-server login times

Use this command to set the number of login attempts. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login times *time*

no ftp-server login times

default ftp-server login times

Parameter Description

Parameter	Description
time	Sets the number of login attempts, in the range from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide The number of login attempts refers to the maximum count you are allowed to perform authentication. If the number of your login attempts exceeds 3, you will be forced offline.

Configuration Examples The following example sets the number of login attempts to 5.

```
Hostname(config)# ftp-server login times 5
```

The following example restores the default setting.

```
Hostname(config)# no ftp-server login times
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.4 ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** form of this command to restore the default setting.

ftp-server timeout *time*

no ftp-server timeout

Parameter Description

Parameter	Description
time	Sets the session idle timeout, in the range from 1 to 3600 in the unit of minutes.

Defaults The default is 10 minutes.

Command Mode Global configuration mode.

Usage Guide Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems

the session connection is invalid and disconnects with the user.

⚠ The session idle time refers to the time for the FTP session between two FTP operations

Configuration Examples The following example sets the session idle timeout to 5 minutes:

```
Hostname(config)# ftp-server timeout 5
```

The following example restores the default setting.

```
Hostname(config)# no ftp-server timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.5 ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** form of this command to restore the default setting.

ftp-server topdir *directory*

no ftp-server topdir

Parameter Description

Parameter	Description
directory	Sets the top-directory.

Defaults No top-directory is configured by default.

Command Mode Global configuration mode.

Usage Guide The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified.
Without this command configured, FTP client fails to access to any file or directory on the FTP server.

Configuration Examples The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory.

```
Hostname(config)# ftp-server topdir /syslog
```

```
Hostname(config)# ftp-server enable
```

The following example restores the default setting.

```
Hostname(config)# no ftp-server topdir
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.6 ftp-server username password

Use this command to set the login username and password for the FTP server. Use the **no** form of this command to restore the default setting.

ftp-server username *username* **password** [*type*] *password*

no ftp-server username *username*

default ftp-server username *username*

Parameter Description

Parameter	Description
username	Sets the login username.
password	Sets the log password

Defaults No username or password is set by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided.

The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. Up to 10 usernames can be configured for the FTP server.

The password must contain letters or numbers. Spaces before or behind the password are allowed but will be ignored. The spaces within are part of the password.

The plaintext password is in the range from 1 to 25 characters. The encrypted password is in the range from 4 to 52 characters.

⚠ The anonymous user login is not supported on the FTP server. The client fails to pass the identity verification if the username is removed.

Configuration Examples The following example sets the username to user:

```
Hostname(config)# ftp-server username user password pass
```

The following example restores the default setting:

```
Hostname(config)# no ftp-server username user
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.7 show ftp-server

Use this command to show the status information of the FTP server.

show ftp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The FTP server status information includes:

- Enabled/Disabled server
- The FTP server top directory
- The FTP server user information, including username, password and connection number. If connection is set up, the IP address, port, transmission type, active/passive mode is shown

Configuration Examples The following example displays the related status information of the FTP server:

```
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]
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7 FTP Client Commands

7.1 copy flash

Use this command to upload the file from the server to the device through FTP Client.

copy flash:[*local-directory/*] *local-file* **ftp:**//*username:password@dest-address* [/*remote-directory*] /*remote-file*

Parameter Description

Parameter	Description
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file".

```
Hostname#                    copy                    flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 copy ftp

Use this command to download the file from the server to the device through FTP Client.

copy ftp://*username:password@dest-address* [/*remote-directory*] / *remote-file* **flash:**[*local-directory*/] *local-file*]

Parameter Description

Parameter	Description
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory "home" on the local device, and changes the name to "local-file".

```
Hostname# copy ftp://user:pass@192.168.23.69/root/remote-file flash:home/local-file
```

The following example uploads the local-file file under directory "home" on the local device to the directory "root" on FTP Server and changes the name to "remote-file".

```
Hostname# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
copy tftp	Uses the TFTP protocol to transfer files.

Platform Description N/A

7.3 ftp-client ascii

Use this command to use ASCII mode for FTP transfer.
Use the **no** form of this command to restore the default setting.
ftp-client ascii
no ftp-client ascii
default ftp-client

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default FTP transfer mode is binary.

Command Mode Global configuration mode

Usage Guide The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples

The following example configures ASCII FTP transfer.

```
Hostname(config)# ftp-client ascii
```

The following example configures binary FTP transfer.

```
Hostname(config)# no ftp-client ascii
```

The following example restores the default setting of the FTP Client.

```
Hostname(config)# default ftp-client
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.4 ftp-client port

Use this command to configure PORT mode used for FTP data connection. Use the **no** form of this command to restore the default setting.

ftp-client port

no ftp-client port

default ftp-client

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default is PASV mode for FTP data connection.

Command Mode

Global configuration mode.

Usage Guide

This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client.

The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples

The following example configures PORT mode used for FTP data connection

```
Hostname(config)# ftp-client port
```

The following example configures PASV mode for FTP data connection.

```
Hostname(config)# no ftp-client port
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

7.5 ftp-client source-address

Use this command to bind FTP Client with the source IP address of client and use this IP address to communicate with server. Use the **no** form of this command to disable source IP address binding. Use the **default** form of this command to restore the default setting.

ftp-client source-address {*ip-address* **|** *ipv6-address*}

no ftp-client source-address

default ftp-client

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the IP address is not bound with the client locally. Instead, it is selected by the route.

Command Mode Global configuration mode

Usage Guide The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples The following example binds FTP Client with source IP address 192.168.23.236.

```
Hostname(config)# ftp-client source-address 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Hostname(config)# ftp-client source-address 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Hostname(config)# no ftp-client source-address
```

The following example restores the default setting of the FTP Client.

```
Hostname(config)# default ftp-client
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

8 TFTP Server Commands

8.1 tftp-server enable

Use this command to enable the TFTP server.

Use the **no** form of this command to disable the TFTP server.

tftp-server enable

no tftp-server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The TFTP server is disabled by default.

Command Modes Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the TFTP server and sets the top directory of the TFTP server to **/syslog**.

```
Hostname(config)# tftp-server topdir /syslog
Hostname(config)# tftp-server enable
```

The following example disables the TFTP server.

```
Hostname(config)# no tftp-server enable
```

Platform Description N/A

8.2 tftp-server topdir

Use this command to configure the top directory for TFTP clients.

Use the **no** or **default** form of this command to restore the default setting.

tftp-server topdir *directory*

no tftp-server topdir

default tftp-server topdir

Parameter Description

Parameter	Description
directory	The top directory for TFTP clients to access. "/" means the root directory.

Defaults The top directory is **flash**:.

Command Modes Global configuration mode

Usage Guide The top directory on the TFTP server defines what files and folders the client is able to access. And the client cannot access the TFTP server before a top directory is correctly configured for the server.

Configuration Examples The following example enables the TFTP servicer and sets the top directory for TFTP clients to **/syslog**.

```
Hostname(config)# tftp-server topdir /syslog
Hostname(config)# tftp-server enable
```

The following example restores the default top directory.

```
Hostname(config)# no tftp-server topdir
```

Platform Description N/A

9 Network Connectivity Test Tool Commands

9.1 clear rping table all

Use this command to clear Rping entries.

clear rping table [**all |** [**ping-object** *owner test-name*] | [**trace-object** *owner test-name*]]

Parameter Description

Parameter	Description
owner	User index
test-name	Test index

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all Rping entries.

```
Hostname# clear rping table all
```

The following example clears the specified Rping entry.

```
Hostname# clear rping table user test
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.2 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**]] [**interval** *millisecond*]]]

Parameter Description

Parameter	Description

address	Specifies an IPv4 address.
length	Specifies the length of the packet to be sent (range: 36-18024, default: 100).
times	Specifies the number of packets to be sent (range:1-4294967295).
seconds	Specifies the timeout time (range: 1-10 seconds).
data	Specifies the data to fill in.
source	Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
df-bit	Sets the DF bit for the IP address. DF bit=1 indicates not to segment the datagrams. By default, the DF bit is 0.
validate	Sets whether to validate the reply packets or not.
detail	Sets whether to contain details in the echoed message. By default, only "!" and "." are displayed.
millisecond	Specifies the ping interval, in the range from 10 to 300000 milliseconds. Default: 100 milliseconds.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command Mode Privileged EXEC mode.

Usage Guide If the device can be pinged, the response information is displayed, and the statistics is listed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configuration Examples The following example tests the connectivity of a network to locate the network connectivity problem.

(Products do not support the VRF parameter. The following example is for reference purpose. Please take the actual device as the standard.)

The following example displays regular ping.

```
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 displays details.

```
Hostname#ping 192.168.21.26 detail
*Apr 16 09:16:08: %PING-7-DEBUG: Ping vrf index -1.
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
```

```
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

The following example tests the connectivity of a network to locate the network connectivity problem (extension ping).

```
Hostname# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
ping 192.168.21.26 length 1500 ntimes 20 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
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=3ms 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 (20/20), round-trip min/avg/max = 1/1/3 ms
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.3 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [**ipv6**] [*ip-address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** *millisecond*]]

Parameter Description	Parameter	Description
	Ipv6-address	Specifies an IPv6 address.
	length	Specifies the length of the packet to be sent (range: 36-18024, default: 100).
	times	Specifies the number of packets to be sent (range:1-4294967295).
	seconds	Specifies the timeout time (range: 1-10 seconds).
	data	Specifies the data to fill in.
	source	Specifies the source IPv6 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
	detail	Sets whether to contain details in the echoed message. By default, only “!” and “.” are displayed.
	millisecond	Specifies the ping interval, in the range from 10 to 300000 milliseconds. Default: 100 milliseconds.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time 2 seconds by default

Command Mode Privileged EXEC mode.

Usage Guide If the device can be pinged, the response information is displayed, and the statistics is listed at the end. If the response data does not match the request data, a ‘Request receive error.’ message is displayed and the statistics is listed in the end. For the extension functions of ping ipv6, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain

name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configuration Examples The following example tests the connectivity of a network to locate the network connectivity problem.

```
Hostname# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, 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 example below shows the extension ping ipv6.

```
Hostname# ping  ipv6 2000::1  length 1500 ntimes 100 timeout 3 data ffff source
192.168.4.10:
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.4 show rping detail

Use this command to display Rping information.

show rping detail

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the Rping information such as numbers of test accounts and users.

Configuration Examples The following example displays Rping information.

```
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
```

Field	Description
Total owner number	The number of users
Total test number	The number of Rping accounts
owner	Username
test name	Test name
storage type	Storage type

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.5 traceroute

Use this command to display all gateways passed by the test packets from the source address to the destination address.

traceroute [**ip**] [*address* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]]

Parameter Description

Parameter	Description
Ipv4-address	Specifies an IPv4 address.
num	Specifies the number of probe packets to be sent (range: 1-255).
source	Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
seconds	Specifies the timeout time (range: 1-10 seconds).
minimum maximum	Specifies the minimum and maximum TTL values (range:1-255).

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Mode Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

Usage Guide Use the **traceroute** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples of the application bout traceroute, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
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      192.168.9.2      4 msec   4 msec   4 msec
6      202.101.143.154      12 msec  8 msec   24 msec
7      61.154.22.36     12 msec  8 msec   22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Hostname# traceroute 202.108.37.42
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
8     218.85.157.222    12 msec   12 msec  12 msec
9      218.85.157.130   16 msec   16 msec  16 msec
10     218.85.157.77    16 msec   48 msec  16 msec
11     202.97.40.65     76 msec   24 msec  24 msec
12     202.97.37.65     32 msec   24 msec  24 msec
13     202.97.38.162    52 msec   52 msec  224 msec
```

```
14     202.96.12.38     84 msec   52 msec  52 msec
15     202.106.192.226  88 msec   52 msec  52 msec
16     202.106.192.174      52 msec   52 msec  88 msec
17     210.74.176.158   100 msec  52 msec  84 msec
18     202.108.37.42    48 msec   48 msec  52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

The following example describes how to use the domain name function:

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.6 traceroute ipv6

Use this command to display all gateways passed by the test packets from the source address to the

destination address.

traceroute [[**ipv6** *ipv6*] [*address* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]]

Parameter Description

Parameter	Description
ipv6-address	Specifies an IPv6 address.
probe *number*	Specifies the number of probe packets to be sent.
source *source*	Specifies the source IPv4 address or source interface of the packet. The loopback interface address (for example, 127.0.0.1) cannot be used as the source address.
timeout *seconds*	Specifies the timeout time.
ttl *minimum maximum*	Specifies the minimum and maximum TTL values.

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Mode Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

Usage Guide Use the **traceroute ipv6** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples of the application bout traceroute ipv6, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
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
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
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     * * *
```

```
5     3004::1        4 msec  28 msec  12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10 TCP Commands

10.1 ip tcp keepalive

Use this command to enable the TCP keepalive function. Use the **no** form of this command to restore the default setting.

ip tcp keepalive [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

no ip tcp keepalive

Parameter Description

Parameter	Description
interval *num1*	The interval of sending the keepalive packet, in the range from1 to 120 in the unit of seconds, The default is 75.
times *num2*	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
idle-period *num3*	Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900.

Defaults The function is disabled by default.

Command Mode Global configuration mode

Usage Guide The keepalive function enables TCP to detect whether the peer end is operating properly.

Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example enables the TCP keepalive function on the device and sets the **idle-period** and **interval** to180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid.

```
Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.2 ip tcp mss

Use this command to set the upper limit of the MSS value. Use the **no** form of this command to restore the default setting.

ip tcp mss *max-segment-size*

no ip tcp mss

Parameter Description

Parameter	Description
max-segment-size	Upper limit of the MSS value in the range from 68 to 10000 bytes

Defaults The default MSS = Outgoing IPv4/v6 MTU- IPv4/v6 header-TCP header.

Command Mode Global configuration mode

Usage Guide This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example sets the upper limit of the MSS value to 1300 bytes.

```
Hostname(config)# ip tcp mss 1300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.3 ip tcp path-mtu-discovery

Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the **no** form of this command to restore the default setting.

ip tcp path-mtu-discovery [**age-timer** *minutes* **| age-timer infinite**]

no ip tcp path-mtu-discovery [**age-timer** *minutes* **| age-timer infinite**]

Parameter Description

Parameter	Description
age-timer *minutes*	The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10.
age-timer infinite	No further discovery after discovering PMTU

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch.
Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled.
According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval until the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

Configuration Examples The following example enables PMTU discovery.

```
Hostname(config)# ip tcp path-mtu-discovery
```

Related Commands

Command	Description
show tcp pmtu	Shows the PMTU value for the TCP connection.

Platform Description N/A

10.4 ip tcp send-reset

Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the **no** form of this command to disable this function,
ip tcp send-reset
no ip tcp send-reset

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found, However, flooding TCP port unreachable packets pose an attack threat to the device, This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet.

```
Hostname(config)# no ip tcp send-reset
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.5 ip tcp synwait-time

Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the **no** form of this command to restore the default setting.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Parameter Description

Parameter	Description
seconds	Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds.

Defaults The default is 20.

Command Mode Global configuration mode

Usage Guide If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example set the timeout value for SYN packets to 10 seconds.

```
Hostname(config)# ip tcp syntime-out 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.6 ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP connections.
Use the **no** form of this command to restore the default setting.
ip tcp window-size *size*
no ip tcp window-size

Parameter Description

Parameter	Description
size	Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes.

Defaults The default is 65535.

Command Mode Global configuration mode

Usage Guide The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.
The sending buffer is used to buffer the data of application programs. Each byte in the sending buffer has a sequence number, and bytes with sequence numbers acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application programs, thus enhancing the performance. However, increasing the receiving buffer and sending buffer will result in more memory consumption of TCP.
This command is used to change the size of receiving buffer and sending buffer for TCP connections. This command changes both the receiving buffer and sending buffer, and only applies to subsequent connections. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example sets the TCP window size to 16386 bytes.

```
Hostname(config)# ip tcp window-size 16386
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.7 show ipv6 tcp connect

Use this command to display the current IPv6 TCP connection information.

show ipv6 tcp connect [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]

Use this command to display the current IPv6 TCP connection statistics.

show ipv6 tcp connect statistics

Parameter Description

Parameter	Description
local-ipv6 *X:X:X:X::X*	Local IPv6 address
local-port *num*	Local port
peer-ipv6 *X:X:X:X::X*	Peer IPv6 address
peer-port *num*	Peer port
statistics	Displays IPv6 TCP connection statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv6 TCP connection information.

```
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 current IPv6 TCP connection statistics.
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        1
CLOSING       0
Total: 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.8 show ipv6 tcp pmtu

Use this command to display information about IPv6 TCP PMTU.

show ipv6 tcp pmtu [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]

Parameter Description	Parameter	Description
	local-ipv6 *X:X:X:X::X*	Local IPv6 address
	local-port *num*	Local port
	peer-ipv6 *X:X:X:X::X*	Peer IPv6 address
	peer-port *num*	Peer port

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example information about IPv6 TCP PMTU.

```
Hostname# show ipv6 tcp pmtu
Number  Local Address          Foreign Address       PMTU
1       1000::1:23             1000::2.13560
```

Field	Description
Number	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.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.9 show ipv6 tcp port

Use this command to display the current IPv6 TCP port status.

show ipv6 tcp port [*num*]

Parameter Description

Parameter	Description
num	Port number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv6 TCP port status.

```
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
```

Field	Description
Number	Number
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.10 show tcp connect

Use this command to display basic information about the current TCP connections.

show tcp connect [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]

Use this command to display the current IPv4 TCP connection statistics.

show tcp connect statistics

Parameter Description

Parameter	Description
local-ip *a.b.c.d*	Local IP address.
local-port *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.
statistics	Displays IPv4 TCP connection statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv4 TCP connection information.

```
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
```

Field	Description
Number	Sequence number.
Local Address	The Local address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
Foreign Address	The remote address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the

	FIN packet.
Process name	Process name.

The following example displays the current IPv4 TCP connection statistics.

```
Hostname#show 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        1
CLOSING       0
Total: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.11 show tcp parameter

Use this command to show TCP parameters.

show tcp parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows TCP parameters.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.12 show tcp pmtu

Use this command to display information about TCP PMTU.

show tcp pmtu [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]

Parameter Description

Parameter	Description
local-ip *a.b.c.d*	Local IP address.
local-port *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays PMTU of IPv4 TCP connection.

```
Hostname# show tcp pmtu
Number  Local Address          Foreign Address       PMTU
1      192.168.195.212.23     192.168.195.112.13560  1440
```

Field	Description
Number	Sequence number.
Local Address	The local address and the port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
Foreign Address	The remote address and the port number. The number after the last "." is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
PMTU	PMTU value.

Related Commands

Command	Description
ip tcp path-mtu-discovery	Enables the TCP PMTU discovery function.

Platform Description N/A

10.13 show tcp port

Use this command to display information about the current TCP port.

show tcp port [*num*]

Parameter Description

Parameter	Description
num	Port number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv4 TCP port status.

```
Hostname#sh tcp port
tcp port status:
Tcpv4 listen on 2650 have connections:
TCB       Foreign Address                      Port    State
Tcpv4 listen on 2650 have total 0 connections.
Tcpv4 listen on 23 have connections:
TCB       Foreign Address                      Port    State
c340800    1.1.1.2                            64571   ESTABLISHED
Tcpv4 listen on 23 have total 1 connections.
Tcpv6 listen on 23 have connections:
TCB       Foreign Address                      Port    State
c429980    3000::2                            64572   ESTABLISHED
```

Tcpv6 listen on 23 have total 1 connections.

Field	Description
TCB	The control block's location in the current memory
Foreign Address	Remote address
Port	Remote port number
State	Status of the current TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent. SYNRCVD: In the three-way handshake phase when the SYN packet has been received.

	ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.14 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.

show tcp parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows TCP parameters.

```
Hostname#show tcp statistics
TCP Packets
  Received: 1103
```

```
  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
Time-wait
  Time-wait bucket table overflow: 0
```

Field Description

Field	Description
TCP Packets	Normal packets and error packets
Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
Time-wait	Session in TIMEWAIT state

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11 IPv4/IPv6 REF Commands

11.1 clear ip ref packet statistics

Use this command to clear IPv4 Ruijie Express Forwarding (REF) packet statistics.

clear ip ref packet statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv4 REF packet statistics.

```
Hostname #clear ip ref packet statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

clear ipv6 ref packet statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv6 REF packet statistics.

```
Hostname #clear ipv6 ref packet statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.3 show ip ref adjacency

Use this command to display the information about the specified adjacent node or all adjacent nodes.

show ip ref adjacency [**glean** | **local** | *ip-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]

Parameter Description

Parameter	Description
glean	Aggregate adjacent node, which is used for a direct route
local	Local adjacent node, which is used by the local host
ip	Next-hop IP address
interface_type	Interface type
interface_number	Interface number
discard	Displays discarded adjacent nodes.
statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.

Configuration Examples The following example displays the information about all adjacent nodes in the adjacent node table.

```
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
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
show ip ref route	Displays all route information in the current REF module.

Platform Description N/A

11.4 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

show ip ref exact-route *source_ipaddress dest_ipaddress*

Parameter Description

Parameter	Description
source_ipaddress	Source IP address of the packet
dest_ipaddress	Destination IP address of the packet

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF

Configuration Examples The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```
Hostname# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74  --> 192.168.13.1:
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
```

Description of fields:

Field	Description
id	Adjacency ID
state	Adjacency state: Unresolved Resolved
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.
ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform Description N/A

11.5 show ip ref packet statistics

Use this command to display IPv4 REF packet statistics.

show ip ref packet statistics

Parameter

Parameter	Description

Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays IPv4 REF packet statistics.

```
Hostname #show ip ref pkt-statistic
ref packet statistic:
   bad head       : 0
   lookup fib fail : 0
   local adj      : 0
   glean adj      : 0
   forward        : 0
   redirect       : 0
   punt adj       : 0
   outif not in ef : 0
   ttl expiration  : 0
   no ip routing   : 0
```

Field	Description
total recved	Number of total packets received by REF
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.6 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

show ip ref resolve-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays IPv4 REF resolution information.

```
Hostname#show ip ref resolve-list
IP               res_state flags interface
1.1.1.1           unres    1     GigabitEthernet 0/0
```

Field	Description
IP	IP address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.7 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

show ip ref route [**default** | *ip mask* | **statistics**]

Parameter Description

Parameter	Description

default	Specifies the default route.
ip	Specifies the destination IP address of the route
mask	Specifies the mask of the route.
statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.

Configuration Examples The following example displays all the routing information in the IPv4 REF table.

```
Hostname#show ip ref route
Codes: * - default route
     # - zero route
ip     mask    weight  path-id     next-hop       interface
255.255.255.255 255.255.255.255 1  4   0.0.0.0    Local 0
224.0.0.0       240.0.0.0        1  1   224.0.0.0
224.0.0.0     255.255.255.0    1  4    0.0.0.0    Local 0
192.168.50.0  255.255.255.0     1  6   0.0.0.0 FastEthernet 0/0
192.168.50.255  255.255.255.255 1  2      0.0.0.0
192.168.50.200 255.255.255.255 1 7 192.168.50.200 FastEthernet 0/0
192.168.50.122  255.255.255.255 1 4 0.0.0.0        Local 0
192.168.50.78  255.255.255.255 1 9 192.168.50.78  FastEthernet 0/0
```

Field	Description
ip	Destination IP address
mask	Mask
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Egress

Related Commands

Command	Description
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.

Platform Description N/A

11.8 show ipv6 ref adjacency

Use this command to display the information about the IPv6 adjacent node.

show ipv6 ref adjacency [**glean** | **local** | *ipv6-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]

Parameter Description

Parameter	Description
glean	Aggregate adjacent node, which is used for a direct route
local	Local adjacent node, which is used by the local host
ipv6-address	Next-hop IP address
interface_type	Interface type
interface_number	Interface number
discard	Displays discarded adjacent nodes.
statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.

Configuration Examples The following example displays the information about the IPv6 adjacent node..

```
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
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node

chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.9 show ipv6 ref exact-route

This command is used to display the IPv6 REF exact route.

show ipv6 ref exact-route *source-ipv6-address destination-ipv6-address*

Parameter Description

Parameter	Description
source-ipv6-address	Source IP address of the packet
destination-ipv6-address	Destination IP address of the packet

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.

```
Hostname#show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2:
ID  state      type    rfct chg ip interface           linklayer(header data)
3   unresolve   glean   1    0   :: GigabitEthernet 0/0
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved

type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.10 show ipv6 ref packet statistics

Use this command to display IPv6 REF packet statistics.

show ipv6 ref packet statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays IPv6 REF packet statistics.

```
Hostname#show ipv6 ref packet statistics
ref packet statistic:
   bad head       : 0
   lookup fib fail : 0
   local adj      : 0
   glean adj      : 0
```

```
  forward        : 0
  redirect       : 0
  hop-limit expiration  : 0
  no ipv6 unicast-routing   : 0
```

Field	Description
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.11 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

show ipv6 ref resolve-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays IPv6 REF resolution information.

Examples

```
Hostname#show ipv6 ref resolve-list
IP              res_state flags interface
1000::1          unres    1     GigabitEthernet 0/0
```

Field	Description
IP	IPv6 address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.12 show ipv6 ref route

Use this command to display all the routing information in the IPv6 REF table.

show ipv6 ref route [**default** | **statistics** | **prefix/len**]

Parameter Description

Parameter	Description
default	Specifies the default route.
statistics	Statistics
prefix/len	Displays the route with the specified prefix (X:X:X:X::X/<0-128>).

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display all routing information in the IPv6 REF table.

Configuration Examples The following example displays all the routing information in the REF IPv6 table.

```
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
```

Field	Description
prefix/len	IPv6 prefix and prefix length.
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

IP Routing Commands

1 RIP Commands

2 OSPFv2 Commands

3 RIPng Commands

4 NSM Commands

1 RIP Commands

1.1 auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

auto-summary

no auto-summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic summary of RIP routes is enabled by default

Command Mode Routing progress configuration mode

Usage Guide Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the

following factors:

- The summarized route is always processed preferentially when you query the RIP database.
- Any sub-route is ignored when you query the RIP database, reducing the processing time.
- If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

Configuration Examples The following example disables automatic route summary of RIPv2.

```
Hostname(Hostname(config)# router rip
Hostname(Hostname(config-router)# version 2
Hostname(Hostname(config-router)# no auto-summary
```

Related Commands

Command	Description
version	Defines the RIP software versions: v1 or v2. Both v1 and v2 are supported by default.

Platform Description N/A

1.2 default-information originate

Use this command to generate a default route in the RIP progress. Use the **no** form of this command to delete the generated default route.

default-information originate [**always] [metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
metric *metric-value*	(Optional) The original metric value of the default route with the value range 115 of metric-value.
route-map *map-name*	(Optional) Name of the associated route-map. Route-map is not associated by default.

Defaults No default route is generated by default.

The default metric value is 1.

Command Mode Routing process configuration mode

Usage Guide By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter always configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

For the default route generated by using the ip default-network command, the default-information originate command is required to add the default route to RIP.

Configuration Examples The following example generates a default route to the RIP routing table.

```
Hostname(config-router)# default-information originate always
```

Related Commands

Command	Description
ip rip default-information	Notifies the default route through an interface.
redistribute	Redistributes the routes from other protocols to RIP.

Platform Description N/A

1.3 default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Indicates the default metric value with the range from 1 to 16. If the

	metric value is greater than or equal to 16, the system regards the route as unreachable.

Defaults The default is 1.

Command Mode Routing process configuration mode

Usage Guide This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this value overwrites the metric value defined with default-metric. If this command is not configured, the default value of default-metric is 1.

Configuration Examples The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3.

```
Hostname(Hostname(config)# router rip
Hostname(Hostname(config-router)# default-metric 3
Hostname(Hostname(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the routes from one routing domain to another routing domain.

Platform Description N/A

1.4 distance

Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter Description

Parameter	Description
distance	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
ip-address	Indicates the prefix of the source IP address of the route.
wildcard	Defines the comparison bit of the IP address, where 0 means

	accurate matching and 1 means no comparison.

Defaults The default is 120.

Command Mode Routing process configuration mode

Usage Guide Use this command to set the management distance of the RIP route.
You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

Configuration Examples The following example sets the management distance of the RIP route to 160, and specifies the management distance of the route learned from 192.168.2.1 as 123.

```
Hostname(config)# router rip
Hostname(config-router)# distance 160
Hostname(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.
distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
prefix *prefix-list-name*	Uses the prefix list to filter the routes.
gateway *prefix-list-name*	Uses the prefix list to filter the source of the routes.
interface-type interface-number	(Optional) Applies the distribution list only to a specified interface.

Defaults The distribution list is not defined by default.

Command Mode Routing process configuration mode

Usage Guide To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.
Without any interface specified, the system will process the route update packets received on all the interfaces.

Configuration Examples The following example enables RIP to control the routes received from the Fastethernet 0/0, only permitting the routes starting with 172.16.

```
Hostname(config)# router rip
Hostname(config-router)# network 200.168.23.0
Hostname(config-router)# distribute-list 10 in fastethernet 0/0
Hostname(config-router)# no auto-summary
Hostname(config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

Platform Description N/A

1.6 distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.
distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]
no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL.
prefix *prefix-list-name*	Uses the prefix list to filter routes.
interface	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
connected	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
ospf *process-id*	(Optional) Applies route update advertisement control to only routes

	introduced from OSPF in this distribution list. *process-id* specifies an OSPF instance.
rip	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
static	(Optional) Applies route update advertisement control to only static routes in this distribution list.

Defaults No route update advertisement is configured by default.

Command Mode Routing process configuration mode

Usage Guide If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.

Configuration Examples The following example advertises only the 192.168.12.0/24 route.

```
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-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.
redistribute	Configures route redistribution.

Platform Description N/A

1.7 enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Routing process configuration mode.

Usage Guide As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP.

Configuration Examples N/A

Related Commands

Command	Description
show ip rip	Displays the global configuration of RIP.

Platform Description N/A

1.8 graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	(Optional) Configures the grace period.
grace-period	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the

forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.
The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.

 During the RIP GR period, the network must be stable.

Configuration Examples The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
Hostname(config)# router rip
Hostname(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform Description N/A

1.9 ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the **no** form of this command to restore the default setting.
ip rip authentication key-chain *name-of-keychain*
no ip rip authentication key-chain

Parameter Description

Parameter	Description
name-of-keychain	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

Defaults The keychain is not associated by default.

Command Mode Interface configuration mode

Usage Guide If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails.
RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain.

```
Hostname(config)#interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
```

Meanwhile, use the **key chain** command to define this keychain in global configuration mode.

```
Hostname(config)#key chain ripchain
Hostname(config-keychain)#key 1
Hostname(config-keychain-key)#key-string Hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description N/A

1.10 ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.
ip rip authentication mode { **text | md5** }
no ip rip authentication mode

Parameter Description

Parameter	Description
text	Configures RIP authentication as plaintext authentication.
md5	Configures RIP authentication as MD5 authentication.

Defaults It is plaintext authentication by default.

Command Mode Interface configuration mode

Usage Guide During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.
If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.
RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

```
Hostname(config)#interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

Related Commands

Command	Description
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
key chain	Defines the keychain and enters the keychain configuration mode

Platform Description N/A

1.11 ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext authentication. Use the **no** form of this command to restore the default setting.
ip rip authentication text-password [**0** | **7**] *password-string*
no ip rip authentication text-password

Parameter Description

Parameter	Description
0	Specifies that the key is displayed as plaintext.
7	Specifies that the key is displayed as cipher text.

password-string	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

Defaults No password string of RIP plaintext authentication is configured by default.

Command Mode Interface configuration mode

Usage Guide This command works only in plaintext authentication mode.
To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.
RIPv1 does not support RIP authentication but RIPv2 does.

Configuration Examples The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.

```
Hostname(config)#interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip authentication text-password
hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

Platform Description N/A

1.12 ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.
ip rip default-information { **only** | **originate** } [**metric** *metric-value*]
no ip rip default-information

Parameter Description

Parameter	Description
only	Notifies the default route rather than other routes.
originate	Notifies the default route and other routes.
metric *metric-value*	Specifies the metric value of the default route, in the range from1 to 15.

Defaults No default route is configured by default. The default metric value is 1.

Command Mode Interface configuration mode

Usage Guide After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the **default-information originate** command of the RIP process are configured at the same time, only the default route of the interface is advertised.

RIP will no longer learn the default route notified by the neighbor if any interface is configured with the ip rip default-information command.

Configuration Examples The following example creates a default route which is notified on ethernet0/1 only.

```
Hostname(config)#interface ethernet 0/1
Hostname(config-if-Ethernet 0/1)#ip rip default-information only
```

Related Commands

Command	Description
default-information originate	Generates a default route in the RIP process.

Platform Description N/A

1.13 ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip receive enable

no ip rip receive enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be received through the interface by default.

Command Mode Interface configuration mode

Usage Guide To prevent an interface from receiving RIP packets, use the no form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use

the **default** form of this command to enable the interface to receive the RIP data package.

Configuration Examples The following example prohibits receiving RIP data packages on fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related Commands

Command	Description
ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

1.14 ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults The default behavior depends on the configuration with the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.

Configuration Examples The following example enables receiving both RIPv1 and RIPv2 data packages.

```
Hostname(config)#interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets

	received/sent on the interface.

Platform Description N/A

1.15 ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip send enable

no ip rip send enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be sent through the interface by default.

Command Mode Interface configuration mode

Usage Guide To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

Configuration Examples The following example prohibits sending RIP data packages on fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# no ip rip send enable
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

1.16 ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the **no** form of this command to disable this function.

ip rip send supernet-routes

no ip rip send supernet-routes

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

Configuration Examples The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related Commands

Command	Description
version	Defines the RIP version
ip rip send enable	Enables or disables sending the RIP package on the interface.

Platform Description N/A

1.17 ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the **no** form of this command to restore the default setting.

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults The default behavior depends on the configuration with the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

Configuration Examples The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip send version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interfaces.

Platform Description N/A

1.18 ip rip split-horizon

Use this command to enable split horizon. Use the **no** form of this command to disable this function.
ip rip split-horizon [**poisoned-reverse**]
no ip rip split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

Configuration Examples The following example disables the RIP split horizon function on the interface fastethernet 0/0.

```
Hostname(config)# interface fastethernet 0/1
Hostname(config-if)# no ip rip split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines the IP address of the neighbor of RIP.
validate-update-source	Enables the source address authentication of the RIP route update message.

Platform Description N/A

1.19 ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter Description

Parameter	Description
ip-address	Indicates the IP addresses to be converged.
ip-network-mask	Indicates the subnet mask of the specified IP address for route convergence.

Defaults The RIP routes are automatically converged to the classful network edge by default.

Command Mode Interface configuration mode

Usage Guide The **ip rip summary-address** command converges an IP address or a subnet on a specified port.

RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

Configuration Examples The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0
255.255.0.0
Hostname(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Hostname(config)# router rip
Hostname(config-router)# network 172.16.0.0
Hostname(config-router)# version 2
Hostname(config-router)# no auto-summary
```

Related Commands

Command	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform Description N/A

1.20 ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

ip rip triggered

ip rip triggered retransmit-timer *timer*

ip rip triggered retransmit-count *count*

no ip rip triggered

no ip rip triggered retransmit-timer

no ip rip triggered retransmit-count

Parameter Description

Parameter	Description
retransmit-timer *timer*	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.
retransmit-count *count*	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links.

With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:

- Update Request packets are received.
- RIP routing information is changed.
- Interface state is changed.
- The router is started.

As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.

⚠ The function can be enabled in the case of the following conditions: (a) The interface has only one neighbor. (b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.

⚠ You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.

⚠ Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.

⚠ To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.

⚠ If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.

Configuration Examples The following example enables TRIP and sets the retransmission interval and maximum retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip rip triggered
Hostname(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
Hostname(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related Commands

Command	Description
show ip rip database	Displays the summarized routing information of the RIP database.
show ip rip interface	Displays the RIP interface information.
ip rip split-horizon	Configures RIP split horizon.

Platform Description N/A

1.21 ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default behavior depends on the configuration of the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default of the **version** command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.

Configuration Examples The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received and sent on the interface.

Platform Description N/A

1.22 neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

neighbor *ip-address*

no neighbor *ip-address*

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.

Defaults The neighbor is not defined by default.

Command Mode Routing process configuration mode

Usage Guide By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

Configuration Examples The following RIP advertises routing information to neighbor IP address 192.168.1.2 only.

```
Hostname(config)# router rip
Hostname(config-router)# passive-interface default
Hostname(config-router)# neighbor 192.168.1.2
```

Related Commands

Command	Description
passive-interface	Configures the interface as a passive interface.

Platform Description N/A

1.23 network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the **no** form of this command to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description

Parameter	Description
network-number	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
wildcard	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

Defaults N/A

Command Mode Routing process configuration mode

Usage Guide The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running.
Without the *wildcard* parameter, the system makes the interface IP address within the classful address range join the RIP running.
Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

Configuration Examples The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
Hostname(config)# router rip
Hostname(config-router)# network 192.168.12.0
Hostname(config-router)# network 172.16.0.0 0.0.0.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.24 offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the **no** form of this command to restore the default setting.
offset-list { access-list-number | name } { **in** | **out** } offset [interface-type interface-number]
no offset-list { access-list-number | name { **in** | **out** } offset [interface-type interface-number]

Parameter Description

Parameter	Description
access-list-number	*name*	Specifies the ACL.

in	Modifies the metric of the received routes using the ACL.
out	Modifies the metric of the sent routes using the ACL.
offset	Indicates the offset of changed metric values. The value is in the range from 0 to16.
interface-type	Applies the ACL to a specified interface.
interface-number	Specifies the interface number.

Defaults No offset is specified by default.

Command Mode Routing process configuration mode

Usage Guide If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Configuration Examples The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

```
Hostname(config-router)# offset-list 7 out 7
```

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

```
Hostname(config-router)# offset-list 8 in 7 fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.25 output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

output-delay *delay*

no output-delay

Parameter Description

Parameter	Description
delay	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

Defaults No sending delay is configured by default.

Command Routing process configuration mode

Mode

Usage Guide In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.
However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration Examples The following example sets the delay to send RIP update packets to 30 milliseconds.

```
Hostname(config)# router rip
Hostname(config-router)# output-delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.26 passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.
passive-interface { **default |** *interface-type interface-num* }
no passive-interface { **default |** *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Sets all interfaces to the passive interfaces.
interface-type interface-num	Indicates the interface type and number.

Defaults Interfaces are set to the non-passive interfaces by default.

Command Mode Routing process configuration mode

Usage Guide The **passive-interface default** command sets all interfaces to the passive interfaces. You can use **no passive-interface** *interface-type interface-num* command to set specified interfaces as non-passive interfaces.
After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified

neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

Configuration Examples

The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.

```
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface gigabitEthernet 0/1
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
ip rip send enable	Enables or disables sending RIP packets on the interface.

Platform Description

N/A

1.27 redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.

redistribute { **connected** | **ospf** *process-id* | **static** } [**metric** *metric-value*] [**route-map** *route-map-name*]

no redistribute { **connected** | **ospf** *process-id* | **static** } [**metric** *metric-value*] [**route-map** *route-map-name*]

Parameter Description

Parameter	Description
connected	Is redistributed from a connected route.
ospf *process-id*	Is redistributed from OSPF and specifies an OSPF instance through process-id. The value is in the range from 1 to 65535.
static	Is redistributed from static routes.
metric *metric-value*	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
route-map *route-map-name*	Sets the redistribution filtering rule.

Defaults

By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command Mode Routing process configuration mode

Usage Guide This command is executed to redistribute external routes to RIP.
It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.
The rule of configuring the **no** form of the redistribute command is as follows:
1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.
2. If the **no** form of this command does not specify any parameter, the command must be deleted.


The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

Configuration Examples The following example redistributes static routes to RIP.

```
Hostname(config-router)# redistribute static
```

Related Commands

Command	Description
default-metric *metric*	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

Platform Description N/A

1.28 router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.
router rip
no router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults No RIP process is running by default.

Command Mode Global configuration mode

Usage Guide One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the **async default routing** command on the asynchronous interface.

Configuration Examples The following example creates the RIP routing process and enters the routing process configuration mode.

```
Hostname(config)# router rip
Hostname(config-router)#
```

Related Commands

Command	Description
network (RIP)	Defines the network number of the RIP process.

Platform Description N/A

1.29 show ip rip

Use this command to display the RIP process information.

show ip rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly.

Configuration Examples The following example displays the basic information of the RIP process such as the update time and management distance.

```
Hostname#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 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
    FastEthernet 0/1      2     2
    FastEthernet 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.30 show ip rip database

Use this command to display the route summary information in the RIP routing database.

show ip rip database [*network-number network-mask*] [**count**]

Parameter Description

Parameter	Description
network-number	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
network-mask	Indicates the subnet mask. It must be specified if the network number is specified.
count	(Optional) Displays the abstract of the route statistics in the RIP database.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Configuration Examples The following example displays all converged address entries in the RIP routing database.

```
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, FastEthernet 0/1
192.168.121.0/24    auto-summary
192.168.121.0/24    redistributed
[1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24    auto-summary
192.168.122.0/24
[1] via 192.168.4.22, Serial 0/1  00:28    permanent
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
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, FastEthernet 0/1
```

The following example displays the statistical information summary of various routes in the RIP routing database.

```
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
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently-running routing protocol process.

Platform Description N/A

1.31 show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol.

show ip rip external [**connected** | **ospf** *process-id* | **static**]

Parameter Description

Parameter	Description
connected	Displays redistributed directly-connected routes.
ospf *process-id*	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
static	Displays redistributed static routes.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example displays direct routes redistributed by the RIP process.

```
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
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform Description N/A

1.32 show ip rip interface

Use this command to display the RIP interface information.

show ip rip interface [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the specified interface type and interface number (optional).

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

Configuration Examples The following example displays the RIP interface information.

```
Hostname# show ip rip interface
FastEthernet 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: test
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
```

Related

Command	Description

Commands

show ip rip	Displays the information of the currently running routing protocol process.

Platform Description N/A

1.33 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

show ip rip peer [*ip-address*]

Parameter Description

Parameter	Description
ip-address	(Optional) Displays the IP address of a specified RIP neighbor.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Configuration Examples The following example displays the RIP neighbor information.

```
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
```

⚠ This series does not support BFG. The configuration example is only for reference.

Related Commands

Command	Description
show ip rip	Displays the information of the routing protocol process that is running.

Platform N/A

Description

1.34 timers basic

Use this command to adjust the RIP clock. Use the **no** form of this command to restore the default setting.

timers basic *update invalid flush*

no timers basic

Parameter Description

Parameter	Description
update	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.
invalid	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
flush	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.

Defaults By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

Command Mode Routing process configuration mode

Usage Guide Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the **show ip rip** command.

⚠ If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

Configuration Examples The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status. When another 90s elapses, they will be cleared.

```
Hostname(config)# router rip
Hostname(config-router)# timers basic 10 30 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.35 validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the **no** form of the command to disable this function.

validate-update-source

no validate-update-source

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

Configuration Examples The following example disables verification of the source IP address of the update packet.

```
Hostname(config)# router rip
Hostname(config-router)# no validate-update-source
```

Related Commands

Command	Description
ip split-horizon	Enables split horizon.
ip unnumbered	Defines the IP unnumbered interface.
neighbor (RIP)	Defines the IP address of a RIP neighbor.

Platform Description N/A

1.36 version

Use this command to define the RIP version of a device. Use the **no** form of this command to restore the default setting.

version { **1 | 2** }

no version

Parameter Description

Parameter	Description
1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

Command Mode Routing process configuration mode

Usage Guide This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Configuration Examples The following example configures the RIP version as version 2.

```
Hostname(config)# router rip
Hostname(config-router)# version 2
```

Related Commands

Command	Description
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
show ip rip	Displays RIP information.

Platform N/A

Description

2 OSPFv2 Commands

2.1 area

Use this command to configure the specified OSPF area. Use the **no** form of this command to restore the default setting.

area *area-id*

no area *area-id*

Parameter Description

Parameter	Description
area-id	ID of the OSPF area. The value can be a decimal integer or an IP address.

Defaults No OSPF area is configured by default.

Command Mode Routing process configuration mode

Usage Guide Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based **area authentication, area default-cost, area filter-list, and area nssa** commands.

- Do not remove the OSPF area configuration under the following conditions:
- Virtual links exist in the backbone area. The virtual links must be removed at first.
- The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.

Configuration Examples The following example removes the configuration of OSPF area 2.

```
Hostname(config)# router ospf 2
Hostname(config-router)# no area 2
```

Related Commands

Command	Description
network area	Defines the interface where OSPF runs and the belonging area of the interface.

Platform Description N/A

2.2 area authentication

Use this command to enable OSPF area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.

Defaults No authentication is enabled by default.

Command Mode Routing process configuration mode

Usage Guide The system supports three authentication types:
1) 0, no authentication. The authentication type in the OSPF packet is 0when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used.3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used.
All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the **ip ospf authentication-key** command to configure the plain text authentication password, and the **ip ospf message-digest-key** command to configure the MD5 authentication password in interface configuration mode.

Configuration Examples The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5
backbone
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
```

Related Commands

Command	Description
ip ospf authentication-key	Defines the OSPF plain text authentication password.
ip ospf message-digest-key	Defines the OSPF MD5 authentication

	password.
area virtual-link	Defines a virtual link.

Platform Description N/A

2.3 area default-cost

Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

Parameter	Description
area-id	ID of the stub area or NSSA
cost	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.

Defaults The default is 1.

Command Mode Routing process configuration mode

Usage Guide This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA.

The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area.

The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the **area default-cost** command to modify the LSA cost.

Configuration Examples The following example sets the cost of the default aggregate route to 50.

```
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
```

Related Commands

Command	Description
area stub	Sets an OSPF area as a stub area.
area nssa	Sets an OSPF area as an NSSA.

Platform Description N/A

2.4 area filter-list

Use this command to filter the inter-area routes on the ABR. Use the **no** form of this command to restore the default setting.

area *area-id* **filter-list** { **access** *acl-name*| **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

Parameter Description

Parameter	Description
area-id	Area ID
acl-name	Name of an Access Control List (ACL)
prefix-name	Prefix-list name
in | **out**	Applies the ACL rule to the routes incoming/outgoing the area.

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide This command can be configured only on an ABR.
You can use this command when it is required to filter the inter-area routes on the ABR.

Configuration Examples The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.5 area nssa

Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the **no** form of this command to delete the NSSA or the NSSA configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*]

[**metric-type** *type*]] [**no-summary**] [**translator** {**stability-interval** *seconds* | **always** }]
no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*]
[**metric-type** *type*]] [**no-summary**] [**translator** { **stability-interval** | **always** }]

Parameter Description

Parameter	Description
area-id	NSSAID
no-redistribution	Imports the routing information to a common area other than the NSSA for the NSSA ABR.
default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
metric *value*	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric-type *type*	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval *seconds*	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to change to a non-translator. The range is from 0 to 2147483647. The default value is 40.
always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.

Defaults No NSSA is defined by default.

Command Mode Routing process configuration mode

Usage Guide The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1.

If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be

removed from the autonomous domain.
To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires.
In a same NSSA, you are recommended to configure the **translator always** parameter on only one ABR.

Configuration Examples The following example sets area 1 as an NSSA on all routers of the area.

```
Hostname(config)#router ospf1
Hostname(config-router)#network 172.16.0.0 0.0.255.255 area0
Hostname(config-router)#network 192.168.12.0 0.0.0.255 area 1
Hostname(config-router)# area1nssa
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.

Platform Description N/A

2.6 area range

Use this command to configure inter-area route aggregation for OSPF. Use the **no** form of this command to delete route aggregation. Use the **no** form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.
area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [c**ost** *cost*]
no area *area-id* **range** *ip-address net-mask* [cost]

Parameter Description

Parameter	Description
area-id	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
ip address net-mask	Network segment whose routes are to be aggregated
advertise | not-advertise	Whether to advertise the aggregate route
cost *cost*	Sets the priority of the interface. The range is from 0 to 16777215.

Defaults No inter-area route aggregation is configured by default.
The configured aggregation range is advertised by default.
The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.

Command Mode Routing process configuration mode

Usage Guide This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default.
You can use the cost option to set the metric of the aggregate route.
You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks.
The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.

Configuration Examples The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

```
Hostname(config)#router ospf 1
Hostname(config-router)#network 172.16.0.0 0.0.15.255area0
Hostname((config-router)#network 172.16.17.0 0.0.15.255area1
Hostname(config-router)#area1range 172.16.16.0 255.255.240.0
```

Related Commands

Command	Description
discard-route	Enables a discarded route to be added to a routing table.
summary-address	Configures the OSPF external route aggregation.

Platform Description N/A

2.7 area stub

Use this command to set an OSPF area as a stub area or full stub area. Use the **no** form of this command to restore the default setting.
area *area-id* **stub** [**no-summary**]
no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
area-id	Stub area ID
no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Defaults No stub area is defined by default.

Command Mode Routing process configuration mode

Usage Guide All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR.

To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.

Configuration Examples The following example sets area 1 as the stub area on all devices in area 1.

```
Hostname(config)# router ospf1
Hostname(config-router)# network172.16.0.0 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
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

Platform Description N/A

2.8 area virtual-link

Use this command to define the OSPF virtual link in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval** *{ seconds* | **minimal hello-multiplier** *multiplier }*] [**hello-interval** *seconds]* [**retransmit-interval** *seconds]* [**transmit-delay** *seconds*] [[**authentication-key** [**0|7**] *key*] | [**message-digest-key** *key-id* **md5** [**0|7**] *key*]]

no area *area-id* **virtual-link** *router-id* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [[**authentication-key**] | [**message-digest-key** *key-id]]*

Parameter Description

Parameter	Description
area-id	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
router-id	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
dead-interval *seconds*	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647.This value must be consistent with that of the neighbor.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
multiplier	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
hello-interval *seconds*	(Optional)Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from1 to 65535.This value must be consistent with that of the neighbor.
retransmit-interval *seconds*	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to 65535. The parameter setting must consider the round-trip time of packets on the link.
transmit-delay *seconds*	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive period reaches a threshold, the LSA will be refreshed.
authentication-key [0|7]*key*	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
message-digest-key *key-id***md5 [0|7]***key*	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults The following are the default values:
dead-interval: 40seconds
hello-interval: 10seconds
retransmit-interval: 5seconds
transmit-delay: 1second

authentication: null
The Fast Hello function is disabled by default.
The other parameters do not have default values.

Command Mode Routing process configuration mode

Usage Guide A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA.
The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID.
The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode.
OSPF supports the Fast Hello function.
If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.
The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link.
No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link.
For the Fast Hello function, you can only configure either the **dead-interval minimal hello-multiplier** parameter or the **hello-interval** parameter.

Configuration Examples The following example sets area 1 as the transition area to establish virtual link with neighbor *2.2.2.2.*

```
Hostname(config)# router ospf 1
Hostname(config-router)# network 172.16.0.0 0.0.15.255 area0
Hostname(config-router)# network 172.16.17.0 0.0.15.255 area1
Hostname(config-router)#area1 virtual-link2.2.2.2
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor *1.1.1.1*. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication inMD5 mode.

```
Hostname(config)# routerospf1
Hostname(config-router)# network172.16.17.0 0.0.15.255area1
```

```
Hostname(config-router)# network172.16.252.0 0.0.0.255 area10
Hostname(config-router)# area 0 authentication message-digest
Hostname(config-router)# area1virtual-link
1.1.1.1message-digest-key1md5hello
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3.

```
Hostname(config)# routerospf1
Hostname(config-router)# network172.16.17.0 0.0.15.255 area1
Hostname(config-router)# network 172.16.252.0 0.0.0.255 area10
Hostname(config-router)# area1 virtual-link1.1.1.1dead-interval minimal
hello-multiplier 3
```

Related Commands

Command	Description
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Displays the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform Description N/A

2.9 auto-cost

Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
ref-bw	Reference bandwidth, in the range from1 to 4294967 Mbps.

Defaults The default is 100Mbps.

Command Mode Routing process configuration mode

Usage Guide By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.

Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps.

Run the **bandwidth** command to set the interface bandwidth.

The costs of OSPF interfaces on several typical lines are as follows:
64Kbps serial line: The cost is 1562.
E1 line: The cost is 48.
10M Ethernet: The cost is 10.
100M Ethernet: The cost is 1.
If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Examples The following example configures the reference bandwidth as 10 Mbps.

```
Hostname(config)# routerospf1
Hostname(config-router)# network172.16.10.0 0.0.0.255 area0
Hostname(config-router)# auto-costreference-bandwidth10
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information
ip ospf cost	Sets the cost value of the OSPF interface.
bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.

Platform Description N/A

2.10 capability opaque

Use this command to enable Opaque LSA. Use the **no** form of this command to disable this function.
capability opaque
no capability opaque

Parameter Description

Parameter	Description
N/A	N/A

Defaults Opaque LSA is enabled by default.

Command Mode Routing process configuration mode.

Usage Guide N/A

Configuration Examples The following example disables Opaque LSA capability.

```
Hostname(config)# router ospf 1
Hostname(config-router)# no capability opaque
```

Related Commands

Command	Description
show ip ospf	Displays the global configuration of OSPF.

Platform Description N/A

2.11 capability vrf-lite

Use this command to disable loop detection for the OSPF instance associated with the VRF.
capability vrf-lite [**auto**]

Use the no form of this command to enable loop detection for the OSPF instance associated with the VRF
no capability vrf-lite [**auto**]

Parameter Description

Parameter	Description
auto	The OSPF instance bound to VRF automatically determines whether it supports the loop detection function.

Defaults By default, The OSPF instance bound to VRF supports the loop detection function.

Command Mode Routing process configuration mode

Default Level 14

Usage Guide This command only takes effect for OSPF instance bound to VRF

By default, the OSPF instance bound to VRF automatically determines whether it supports the loop detection function and PE-CE OSPF features.

- Run the **capability vrf-lite** command to forcibly disable the function.
- Run the **no capability vrf-lite** command to forcibly enable the function.
- Run the **capability vrf-lite auto** command to enable the OSPF instance bound to VRF to automatically determines whether the function is to be enabled.
- Run the **default capability vrf-lite auto** command to restore default configuration.

The loop detection function of OSPF instance can prevent possible routing loops of VPN. When an OSPF instance bound to VRF receives an LSA, the LSA will be processed according to the following principles:

- If the loop detection function is disabled, the OSPF protocol will not detect the DN bit and VPN domain tag in the LSA message after receiving the LSA message, and will let the LSA participate in the OSPF calculation.
- LSA Type 3, Type 5 and Type 7: The OSPF protocol will detect DN bit. If the received LSA has DN bit,

the LSA will not participate in OSPF calculation.

- LSA Type 5 and Type 7: The OSPF protocol will detect VPN Domaintag. If the VPN domain flag of the received LSA is the same as that of the local OSPF instance, the LSA will not participate in OSPF calculation.

The PE-CE OSPF feature is to convert different OSPF LSAs and advertise them to CE according to the BGP extension attribute of the route (see Section MPLS L3VPN in the *MPLS Configuration Guide* for the PE-CE OSPF feature). If this feature is disabled, different OSPF LSAs will not be converted according to the BGP attribute.

By default, the OSPF instance bound to VRF automatically determines whether it supports the loop detection function. The purpose of this function is described as follows.

In some application scenarios, you may want to disable the loop detection function of VRF OSPF instances. For example, VPN users use MCE devices and PEs to interact with VPN routes. If the OSPF protocol is used between MCE and PEs to interact with VPN routes, then in order for MCEs to learn the VPN routes published by PEs and publish them to the downstream VPN sites, you need to disable the loop detection function of VRF OSPF instances of MCE devices. At present, for general MCE scenarios, the device can automatically judge and disable the loop detection feature of the OSPF instance. If the automatic judgment is incorrect, you can run the [**no**] **capability vrf-lite** command to forcibly disable or enable the loop detection feature of the OSPF instance.

Configuration Examples

The following example disables loop detection under the OSPFinstance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router ospf 10 vrf vpn1
Hostname(config-router)# capability vrf-lite
```

Verification

N/A

Prompt Messages

The following message is displayed if the OSPF instance is not bound to VRF.

```
% The command CAN NOT apply to ospf instance bound to VRF default.
```

Common Errors

N/A

Platform Description

N/A

2.12 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf *(process-id)* **process**

Parameter Description

Parameter	Description

process-id	OSPF instance ID. When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance. When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.

Defaults The rule recommended in the RFC 1583 is used by default.

Command Mode Privileged EXEC mode

Usage Guide Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.

Configuration Examples The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

```
Hostname#clearipospf1process
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 compatible rfc1583

Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS).

compatible rfc1583

no compatible rfc1583

Parameter Description

Parameter	Description
N/A	N/A

Defaults The RFC 1583 rule is used by default.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration The following example determines the best route with the RFC 2328 rule.

Examples

```
Hostname(config)# routerospf1
Hostname(config-router)# nocommpatiblerfc1583
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform Description N/A

2.14 default-information originate

Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to restore the default setting.
default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]
no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric of the default route in the range from0 to 16777214
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
route-map *map-name*	Associated route map name. No route map is associated by default.

Defaults No default route is generated by default.
The default value of metric is 1.
The default value of metric-type is 2.

Command Mode Routing process configuration mode

Usage Guide When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can generate the default route with the **default-information originate** command in routing process configuration mode.
If the always parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the

default route. To make sure whether the default route is generated, use the **show ip ospf database** command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the show ip route command on the OSPF neighbor to display the default route.

The metric of the external default route can be defined only with the **default-information originate** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, 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 area. To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

⚠ The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.

Configuration Examples

The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50.

```
Hostname(config)#routerospf 1
Hostname(config-router)#network172.16.24.0 0.0.0.255 area 0
Hostname(config-router)#default-information originate
alwaysmetric50metric-type1
```

Related Commands

Command	Description
show ip ospf database	Displays OSPF link state database.
show ip route	Displays the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description

N/A

2.15 default-metric

Use this command to set the **default metric** of OSPF redistribution route. Use the **no** form of this command to restore the default setting.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Default metric of the OSPF redistribution route in the range from1 to

	16777214

Defaults The default metric is not configured by default.

Command Mode Routing process configuration mode

Usage Guide The **default-metric** command must work with the **redistribute** command in routing process configuration mode to modify the initial metric of all redistributed routes.
The configuration result of the **default-metric** command does not take effect for the external routes injected into the OSPF routing domain with the **default-information originate** command.

Configuration Examples The following example configures the default metric of the OSPF redistribution route as 50.

```
Switch(config)# router rip
Hostname(config-router)# network192.168.12.0
Switch(config-router)# version 2
Hostname(config-router)# exit
Hostname(config)# routerospf1
Hostname(config-router)# network172.16.10.0 0.0.0.255area0
Switch(config-router)# default-metric 50
Hostname(config-router)# redistribute rip subnets
```

Related Commands

Command	Description
redistribute	Redistributes the routes of other routing processes.
show ip ospf	Displays the OSPF global configuration information.

Platform Description N/A

2.16 discard-route

Use this command to enable adding the discard-route into the core route table. Use the **no** form of this command to disable this function.
discard-route { **internal | external** }
no discard-route { **internal** | **external** }

Parameter Description

Parameter	Description
internal	Enables adding the discard-route generated with the area range command
external	Enables adding the discard-route generated with the

	summary-address command.

Defaults Adding the discard-route is enabled by default.

Command Mode Routing process configuration mode

Usage Guide After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The discard-route is generated automatically and will not be transmitted.

Configuration Examples The following example disables adding the discard routes generated with the area range command.

```
Hostname(config)# router ospf 1
Hostname(config-router)# no discard-route internal
```

Related Commands

Command	Description
area range	Configures the route aggregation between OSPF areas.
summary-address	Configures the route aggregation out of the OSPF routing domain.

Platform Description N/A

2.17 distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

no distance [**ospf**]

Parameter Description

Parameter	Description
distance	Sets the route AD in the range from1 to 255.
intra-area *distance*	Sets the AD of the intra-area route in the range from1 to 255.
inter-area *distance*	Sets the AD of the inter-area route in the range from1 to 255.
External *distance*	Sets the AD of the external route in the range from1 to 255.

Defaults The default value is 110.

The default intra-area distance is 110.

The default inter-area distance is 110.

The default external distance is 110.

Command Mode OSPF Routing process configuration mode

Usage Guide This command is used to specify different ADs for different types of OSPF routes.

Configuration Examples The following example sets the OSPF external route AD to 160.

```
Hostname(config)# routerospf1
Hostname(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.18 distribute-list in

Use this command to configure LSA filtering. Use the **no** form of this command to restore the default setting.

distribute-list *{ [access-list-number* | *name]* | *prefix prefix-list-name [* **gateway** *prefix-list-name]* | **route-map** *route-map-name } in [interface-type interface-number]*

no distribute-list *{ [access-list-number* | *name]* | *prefix prefix-list-name [* **gateway** *prefix-list-name]* | route-map *route-map-name } in [interface-type interface-number]*

Parameter Description

Parameter	Description
access-list-number | **name**	Uses the ACL filtering rule.
gateway *prefix-list-name*	Uses the gateway filtering rule.
Prefix *prefix-list-name*	Uses the prefix-list filtering rule.
route-map *route-map-name*	Uses the route-map filtering rule.
interface-type interface-number	Configures the LSA route filtering on the interface.

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries

calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR.
The following route-map rules will be supported if the route-map parameter is configured:
match interface
match ip address
match ip address prefix-list
match ip next-hop
match ip next-hop prefix-list
match metric
match tag
Filtering routes by using 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.

Configuration Examples

The following example configures LSA filtering.

```
Hostname(config)# access-list3permit172.16.0.00.0.127.255
Hostname(config)# router ospf 25
Hostname(config-router)# distribute-list 3 in ethernet 0/1
```

Related Commands

Command	Description
distribute-list out	Filters redistribution routes.

Platform Description

N/A

2.19 distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the **redistribute** command. Use the **no** form of this command to restore the default setting.
distribute-list *{ [access-list-number* | *name]* | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* | **rip** | **static**]
no distribute-list *{ [access-list-number* | *name]* | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* | **rip** | **static**]

Parameter Description

Parameter	Description
access-list-number | *name*	Uses the ACL filtering rule.
prefix prefix-list-name	Uses the prefix-list filtering rule.
connected | ospf process-id | **rip | static**	Source of the routes to be filtered

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.

Configuration Examples The following example filters the redistributed static routes.

```
Hostname(config)# routerospf1
Hostname(config)# redistribute static subnets
Hostname(config-router)# distribute-list 22 outstatic
Hostname(config-router)# distribute-list prefix jjj out static
% Access-list filter exists, please de-config first
```

Related Commands

Command	Description
distribute-list in	Configures LSA filtering.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

2.20 enable mib-binding

Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the **no** form of this command to restore the default setting.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MIB is bound with the OSPFv2 process with the smallest ID by default.

Command Mode Routing process configuration mode

Usage Guide OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User

operations take effect for this process.

To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.

Configuration Examples The following example operates OSPFv2 process 100 over SNMP:

```
Hostname(config)# routerospf100
Hostname(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable traps	Configures the OSPF TRAP function.

Platform Description N/A

2.21 enable traps

The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the **no** form of this command to restore the default setting.

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

Parameter	Description
error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches. **Ifauthfailure** — Interface authentication error **Ifconfigerror** — Interface parameter configuration error **Ifrxbadpacket** — Error packets received on the interface **Virtifauthfailure** — Authentication error on the virtual interface

	Virtifconfigerror — Parameter configuration error on the virtual interface **Virtifrxbadpacket** — Error packets received on the virtual interface
isa	Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches. **Lsdbapproachoverflow** — External LSA count has reached the 90% of the upper limit. **Lsdboverflow** — External LSA count has reached the upper limit. **Maxagelsa** — LSA reaching the aging time **Originatelsa** — Generates new LSA
retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches. **Iftxretransmit** — Packet retransmission on the interface **Virtiftxretransmit** — Packet retransmission on the virtual interface
state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches. **Ifstatechange** — Interface state change **NbrRestartHelperStatusChange** — State change during the neighbor GR process **Nbrstatechange** — Neighbor state change **NssaTranslatorStatusChange** — State change of the NSSA translator **RestartStatusChange** — State change of the GR Restarter on the device **Virtifstatechange** — State change on the virtual interface **VirtNbrRestartHelperStatusChange** — Status change of the virtual neighbor GR process **Virtnbrstatechange** — State change on the virtual neighbor

Defaults All TRAP switches are disabled by default.

Command Mode Routing process configuration mode

Usage Guide The **snmp-server enable traps ospf** command must be configured before you configure this command, for it is limited by the **snmp-server** command.
This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration The following example enables all TRAP switches of OSPFv2 process 100.

Examples

```
Hostname(config)# routerospf100
Hostname(config-router)# enable traps
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable mib-binding	Binds the OSPFv2 process with MIB.
snmp-server enable traps ospf	Enables the OSPF TRAP notification function.

Platform Description N/A

2.22 graceful-restart

Use this command to enable the graceful restart (GR) of OSPF on the device. Use the **graceful-restart grace-period** command to configure the grace period parameter and enable the OSPF GR function. Use the **no** form of this command to disable this function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [**graceful-period**]

Parameter Description

Parameter	Description
grace-period *grace-period*	Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s.
inconsistent-lsa-checking	Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations.

The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly.

GR is unavailable when the Fast Hello function is enabled.

Configuration Examples The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

```
Hostname(config)# router ospf 1
Hostname(config-router)# graceful-restart
Hostname(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform Description N/A

2.23 graceful-restart helper

Use this command to enable the graceful restart helper function. Use the **no** form of this command to restore the default setting.

graceful-restart helper disable

no graceful-restart helper disable

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking**}

no graceful-restart helper {**strict-lsa-checking** | **internal-lsa-checking**}

Parameter Description

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 the 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 the GR helper.

Defaults The GR helper is enabled by default.
The router enabled with the GR helper does not check the LSA change by default.

Command Mode Routing process configuration mode

Usage Guide This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for

any device that implements GR.
After a device becomes the 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 **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.

Configuration Examples The following example disables the GF helper and modifies the policy of checking network changes.

```
Hostname(config)# router ospf1
Hostname(config-router)# graceful-restart helper disable
Hostname(config-router)# no graceful-restart helper disable
Hostname(config-router)# graceful-restart helper
strict-lsa-checking
```

Related Commands

Command	Description
graceful-restart	Enables GR on the device.

Platform Description N/A

2.24 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of this command to restore the default setting.
ip ospf authentication [**message-digest** | **null**]
no ip ospf authentication

Parameter Description

Parameter	Description
message-digest	Enables MD5 authentication on the interface.
null	Enables no authentication.

Defaults No authentication mode is configured and that of the local area is used on the interface by default.

Command Mode Interface configuration mode

Usage Guide Plaintext authentication is applicable when **no** option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured

as **null,** no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.

Configuration Examples The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

```
Hostname(config)#interface fastEthernet0/1
Hostname(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related Commands

Command	Description
area authentication	Enables authentication and defines authentication mode in the OSPF area.
ip ospf authentication-key	Configures the plain text authentication key.
ip ospf message-digest-key	Configures the MD5 authentication key.

Platform Description N/A

2.25 ip ospf authentication-key

Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf authentication-key [**0 | 7**] *key*

no ip ospf authentication-key

Parameter Description

Parameter	Description
0	Displays the key in plain text.
7	Displays the key in cipher text.
key	Key containing at most eight characters.

Defaults It is disabled by default.

Command Mode Interface configuration mode

Usage Guide The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key.

To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode.
The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

Configuration Examples The following example configures the OSPF authentication key ospfauth for fast Ethernet *0/1*.

```
Hostname(config)#interfacefastEthernet0/1
Hostname(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode
ip ospf authentication	Enables authentication on the interface and defines authentication mode

Platform Description N/A

2.26 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the **no** form of this command to restore the default setting.
ip ospf cost *cost*
no ip ospf cost

Parameter Description

Parameter	Description
cost	OSPF interface cost in the range from 0 to 65535

Defaults The default interface cost is calculated as follows:
Reference bandwidth/Bandwidth
The reference bandwidth is *100* Mbps by default.

Command Mode Interface configuration mode

Usage Guide By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode.
The default costs of different types of lines are as follows:

- 64K serial line: 1562
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Configuration Examples The following example configures the OSPF cost of fastEthernet 0/1 to100.

```
Hostname(config)# interfacefastEthernet0/1
Hostname(config-if-FastEthernet 0/1)# ipospfcost100
```

Related Commands

Command	Description
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Displays the OSPF global configuration information

Platform Description N/A

2.27 ip ospf database-filter all out

Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the **no** form of the command to restore the default setting.

ip ospf database-filter all out

no ip ospf database-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled and all LSA update packets can be sent on the interface by default.

Command Mode Interface configuration mode

Usage Guide To stop sending LSA update packets on the interface, enable this function on the interface. Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.

Configuration Examples The following example stops sending LSA update packets of fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
```

```
Hostname(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 ip ospf dead-interval

Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf dead-interval { *seconds* **| minimal hello-multiplier** *multiplier* }

no ip ospf dead-interval

Parameter Description

Parameter	Description
seconds	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.
minimal	Indicates that the Fast Hello function is enabled to set the dead interval to 1s.
hello-multiplier *multiplier*	Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.

Defaults The value of dead-interval is 4 times the interval configured with the **ip ospf hello-interval** command by default.

Command Mode Interface configuration mode

Usage Guide The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically.

When using this command to manually modify the dead interval, pay attention to the following issues:

1. The dead interval cannot be shorter than the Hello interval.
2. The dead interval must be the same on all routers in the same network segment.

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 death 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 death interval must be consistent and the **hello-multiplier** values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval.

Run the **show ip ospf virtual-links** command to monitor the death interval and 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.

Configuration Examples

The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to30seconds.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf dead-interval30
```

The following example configures the value of hello-multiplier to3.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Displays OSPF interface information.

Platform Description

N/A

2.29 ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets. Use the **no** form of this command to restore the default setting.

ip ospf disable all

no ip ospf disable all

Parameter Description

Parameter	Description

N/A	N/A

Defaults OSPF packets are generated on the specified interface by default.

Command Mode Interface configuration mode

Usage Guide The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.

Configuration Examples The following example prevents the specified interface from generating OSPF packets.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.30 ip ospf hello-interval

Use this command to set the interval for sending Hello packets in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter Description

Parameter	Description
seconds	Interval for sending Hello packets in seconds. The range is from1 to 65535.

Defaults The defaults are as follows:

10secons for Ethernet

10seconsfor PPP or HDLC encapsulated interfaces

10secons for frame relay PTP interfaces

30secons for non-frame relay PTP sub-interface and X.25 interfaces

Command Mode Interface configuration mode

Usage Guide The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic. The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.

Configuration Examples The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to15.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf hello-interval15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform Description N/A

2.31 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf message-digest-key *key-id* **md5** [**0 | 7**] *key*

no ip ospf message-digest-key *key-id*

Parameter Description

Parameter	Description
key	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
key-id	Key identifier in the range from1 to 255

Defaults No MD5 key is configured by default.

Command Mode Interface configuration mode

Usage Guide The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same

physical network segment must be configured with the same key. For neighbors, the same key identifier must correspond to the same key.

To enable OSPF area authentication, execute the **area authentication** command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

The system supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, the old key can be deleted.

Configuration Examples The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
Hostname(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
Hostname(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5
hello10
Hostname(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# no ip ospf message-digest-key10md5
hello10
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode.
ip ospf authentication	Enables authentication on the interface and defines authentication mode.

Platform Description N/A

2.32 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description packet. Use the **no** form of this command to restore the default setting.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description

Parameter	Description

N/A	N/A

Defaults MTU check is disabled by default.

Command Mode Interface configuration mode

Usage Guide After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples The following example disables the MTU check function on fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.33 ip ospf network

Use this command to configure the OSPF network type in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf network { **broadcast | non-broadcast |**
point-to-multipoint [**non-broadcast**] **| point-to-point** }
no ip ospf network

Parameter Description

Parameter	Description
broadcast	Sets the OSPF network type as the broadcast type.
non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The non-broadcast option means the point-to-multipoint non-broadcast type.
point-to-point	Sets the OSPF network type as the point-to-point type.

Defaults The default configurations are as follows:
PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay

point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation
NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)
Broadcast network type: Ethernet encapsulation
By default, the network type is the point-to-multipoint network type.

Command Mode Interface configuration mode

Usage Guide 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.

Configuration Examples The following example configures the frame relay interface network as the P2P type.

```
Hostname(config)# interface Serial 1/0
Hostname(config-Serial 1/0)#ip address 172.16.24.4 255.255.255.0
Hostname(config-Serial 1/0)# encapsulation frame-relay
Hostname(config-Serial 1/0)# ip ospf network point-to-point
```

The following example configures the frame relay interface network as the NBMA type.

```
Hostname(config)# interface Serial 1/0
Hostname(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
Hostname(config-Serial 1/0)# encapsulation frame-relay
Hostname(config-Serial 1/0)# ip ospf network non-broadcast
Hostname(config-Serial 1/0)#exit
Hostname(config)# router ospf 20
Hostname(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
dialer map ip	Defines the mapping between IP address and dialing number.
frame-relay map	Defines the mapping between IP address and frame DLCI.
neighbor(OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Defines the mapping between IP address and X.25 network address.

Platform Description N/A

2.34 ip ospf priority

Use this command to configure the OSPF priority in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf priority *priority*

no ip ospf priority

Parameter Description

Parameter	Description
priority	Sets the OSPF priority of the interface in the range from 0 to 255.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.

Configuration Examples The following example configures the priority offastethernet 0/1 as 0.

```
Switch(config)#interface fastethernet 0/1
Hostname(config-if-FastEthernet 0/1)# ipospfpriority0
```

Related Commands

Command	Description
ip ospf network	Configures the network type of the interface.

Platform Description N/A

2.35 ip ospf retransmit-interval

Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter Description

Parameter	Description

seconds	Interval for sending the LSU packets in seconds. The range is from 1 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.

Defaults The default is 5.

Command Mode Interface configuration mode

Usage Guide After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSU will be sent once again.
In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the area virtual-link command followed with the keyword retransmit-interval.

Configuration Examples The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description N/A

2.36 ip ospf source-check-ignore

Use this command to disable the source address check in the point-to-point link. Use the **no** form of this command to restore the default setting
ip ospf source-check-ignore
no ip ospf source-check-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need to disable the source address check to ensure the normal establishment of OSPF neighbors. The source address check shall be never enabled, especially for the unnumbered interfaces.

Configuration Examples The following example disables the source address check function in the point-to-point link.

```
Hostname(config)# interface serial 1/0
Hostname(config-if)# ip ospf source-check-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.37 ip ospf transmit-delay

Use this command to define the LSU packet transmission delay in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter Description

Parameter	Description
seconds	LSU packet transmission delay in seconds in the range from 1 to 65535.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the **ip ospf transmit-delay** command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU packet transmission delay of the virtual link is defined with the **area virtual-link** command followed with the keyword retransmit-interval.

The software will resend or request resending the LSA with Age up to 3600. If no update is obtained

in time, the aged LSA will be cleared from the link state database.

Configuration Examples The following example configures the transmission delay of fastEthernet 0/1 as 10.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description N/A

2.38 log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the **no** form of the command to disable this function.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

Parameter	Description
detail	Records the detail of changes.

Defaults This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example logs the neighbor state changes.

```
Hostname(config)# router ospf 1
Hostname(config-router)# log-adj-changes detail
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.

Platform Description N/A

2.39 max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets in the range from1 to 65535

Defaults The default is 5.

Command Mode Routing process configuration mode

Usage Guide When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.

Configuration Examples The following example sets the maximum number of DD packets to 4.
After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Hostname(config)# routerospf10
Hostname(config-router)# max-concurrent-dd4
```

Related Commands

Command	Description
router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.

Platform Description N/A

2.40 max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the **no** form of this command to restore the default setting.

max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup** *[seconds]]* [**summary-lsa** *[max-metric-value]]*

no max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup**

[seconds]] [**summary-lsa** *[max-metric-value]]*

Parameter Description

Parameter	Description
router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
max-metric-value	Maximum metric of the LAS. The range is 1 to 16777215.The default value is 16711680,
include-stub	Configures the maximum metric of the stub links in the Router LSA.
on-startup	Advertises the maximum metric when the routing device starts up.
seconds	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)

Defaults The normal metric LSAs are used by default.

Command Mode Routing process configuration mode

Usage Guide You can run the **max-metric router-lsa** command to set the maximum metric of non-stub links in the Router LSA generated by the routing device. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command configured, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa** parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the **external lsa** parameter to set the external LSA as the maximum metric.

The **max-metric router-lsa** command is usually used in the following scenes:

The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device. In this case, use the **on-startup** parameter to set certain delay, so that this device can serve as a transmission node after restarting.

The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.

Remove the device from the network gracefully. With this command configured, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.

For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links

with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is, no dataflow will be sent to the router that have generated these LSAs.

Configuration Examples The following example configures the LSA maximum metric as 100 seconds after starting the device.

```
Hostname(config)# router ospf 20
Hostname(config-router)# max-metric router-lsa on-startup 100
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF related configurations.

Platform Description N/A

2.41 neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no** form of this command to restore the default setting.

Neighbor *ip-address* [[**poll-interval** *seconds*] [**priority** *priority*] | [**cost** *cost*]]

no neighbor *ip-address* [[**poll-interval**] [**priority**] | [cost]]

Parameter Description

Parameter	Description
ip address	IP address of the neighbor
poll-interval *seconds*	(Optional) Specifies the interval of polling neighbors in seconds. The range is from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
priority *priority*	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
cost *cost*	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports this option.

Defaults No neighbor is defined by default.
The default neighbor polling interval is 120 seconds.
The default NBMA neighbor priority is 0.

Command Mode Routing process configuration mode

Usage Guide The software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.
In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor relationship.
Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.

Configuration Examples The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds.

```
Hostname(config)# routerospf 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
```

Related Commands

Command	Description
ip ospf priority	Sets the interface priority.
ip ospf network	Sets the network type

Platform Description N/A

2.42 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the **no** form of this command to restore the default setting.
network *ip-address wildcard* **area** *area-id*
no network *ip-address wildcard* **area** *area-id*

Parameter Description

Parameter	Description
ip-address	IP address of the interface
wildcard	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.

Defaults No OSPF area is configured by default.

Command Mode Routing process configuration mode

Usage Guide The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area.
To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command. If only the secondary IP address is included, OSPF cannot be enabled on the interface.
You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.

Configuration Examples The following example defines:
Three areas: 0, 1 and 172.16.16.0
The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1
The interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2
The remaining interface being assigned to area 0.

```
Hostname(config)# routerospf 20
Hostname(config-router)# network172.16.16.0
0.0.15.255 area172.16.16.0
Hostname(config-router)# network192.168.12.0
0.0.0.255 area 1
Hostname(config-router)# network0.0.0.0 255.255.255.255 area0
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process.

Platform Description N/A

2.43 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the **no** form of this command to restore the default setting.
overflow database *number* [**hard | soft**]
no overflow database

Parameter Description

Parameter	Description
number	Maximum number of LSAs. The range is from 1 to 4294967294.
hard | soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number.

	soft: issues an alarm when the number of LSAs exceeds that number.

Defaults The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command Mode Routing process configuration mode

Usage Guide To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
Hostname(config)# router ospf 10
Hostname(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.44 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the **no** form of this command to restore the default setting.
overflow database external *max-dbsize wait-time*
no overflow database external

Parameter Description

Parameter	Description
max-dbsize	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
wait-time	Waiting time of the routing device from the overflow status to normal status. The range is from 0 to 2147483647.

Defaults The maximum number of external-LSAs is not restricted by default.
If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.

Command Mode Routing process configuration mode

Usage Guide When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.

⚠ When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:

⚠ The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.

⚠ Incorrect routes occur, including loops.

⚠ AS-External-LSAs may be frequently retransmitted.

Configuration Examples The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds.

```
Hostname(config)# routerospf10
Hostname(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.45 overflow memory-lack

Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Routing process configuration mode

Usage Guide The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and effectively prevent the memory from increasing.

It is possible that enabling this function causes the route loop in the whole network. To reduce that

possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.
Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state.
Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Configuration Examples The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

```
Hostname(config)# router ospf 1
Hostname(config-router)# no overflow memory-lack
```

Related Commands

Command	Description
clear ip ospf process	Resets the OSPF instances.
show ip protocols ospf	Displays the OSPF information.

Platform Description N/A

2.46 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. Use the **no** form of this command to restore the default setting.
passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }
no passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }

Parameter Description

Parameter	Description
interface-type interface-number	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
interface-type interface-number ip-address	Sets the address of the specified interface as a passive address.

Defaults No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.

Command Routing process configuration mode

Mode

Usage Guide To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address

Configuration Examples The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.

```
Hostname(config)# routerospf 30
Hostname(config-router)# passive-interface fastEthernet 0/1
Hostname(config-router)# passive-interface fastEthernet 0/1 1.1.1.1
```

Related Commands

Command	Description
show ip ospf interface	Displays the configuration information of the interface.

Platform Description N/A

2.47 redistribute

Use this command to redistribute the external routing information. Use the **no** form of this command to restore the default setting.

redistribute { **connected** | **ospf** *process-id* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1 | 2**] }] | **rip** | **static** } [**metric** *metric-value*] [**metric-type** { **1** | **2** }] [**route-map** *route-map-name*] [**subnets**] [**tag** *tag-value*]

no redistribute { **connected** | **ospf** *process-id* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1 | 2**] }] | **rip** | **static** } [**metric**] [**metric-type**] [**route-map**] [**subnets**] [**tag**]

Parameter Description

Parameter	Description
connected	Redistribution from direct routes
ospf *process-id*	Redistribution from an ospf instance specified in process-id in the range from 1 to 65,535
external [**1**	**2**]	E1, E2 or all external routes=
internal	Inter-area and intra-area routes
nssa-external [**1**	**2**]	N1, N2 or all external routes outside NSSA
rip	Redistribution from rip
static	Redistribution from static routes
match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
metric *metric-value*	Specifies the metric of an OSPF external LSA in the range from 0 to

	16777214.
metric-type{**1** | **2** }	Sets the external routing type as E-1 or E-2.
route-map *route-map-name*	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag *tag-value*	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.

Defaults

Redistribution configuration is not supported by default.
If you configure OSPF redistribution, all subtype routes of the instance are redistributed.
In other cases, all routings of this type are redistributed.
The default value of metric-type is E-2.
No route-map is associated by default.

Command Mode

Route configuration mode

Usage Guide

After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs.
When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration.
When you filter routes for redistribution by following the route-map rule, the match rule of the route-map rule is specific for the original redistribution parameters. The route-map rule works only when the redistributed OSPF routes follow the match rule.


The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.


The following are the rules for configuring the no form of the redistribute command:1. If the **no** form specifies some parameters, restore their default values.2. If the **no** form contains no parameter, delete the whole command..

Configuration Examples

N/A

Related Commands

Command	Description
summary-address	Configures the aggregate route for the external route of the OSPF route area.
default-metric	Sets the default metric of the OSPF redistribution route.

Platform Description

N/A

2.48 router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to restore the default setting.

router ospf

no router ospf *process-id*

Parameter Description

Parameter	Description
process-id	ID of an OSPF process. If the process ID is not configured, process 1 is configured.

Defaults No OSPF routing process exists by default.

Command Mode Global configuration mode

Usage Guide Based on the original implementation, the system adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples N/A

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.49 router ospf max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

router ospf max-concurrent-dd *number*

no router ospf max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets in the range from 1 to 65535.

Defaults The default is 10.

Command Mode Global configuration mode

Usage Guide When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.

Configuration Examples The following example sets the maximum number of DD packets to 4.
After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Hostname(config)# router ospfmax-concurrent-dd4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.

Platform Description N/A

2.50 router-id

Use this command to set the router ID. Use the **no** form of this command to restore the default setting.
router-id *router-id*
no router-id

Parameter Description

Parameter	Description
router-id	Router ID in IP address form

Defaults The OSPF routing process will select the maximal interface IP address as the router ID by default. If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.

Command Mode Routing process configuration mode

Usage Guide You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not

recommended to change the router ID. The device can be changed only when no LSA is generated.

Configuration Examples The following example modifies the router ID to 0.0.0.36.

```
Hostname(config)# router ospf 20
Hostname(config-router)# router-id0.0.0.36
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.

Platform Description N/A

2.51 show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the information of the OSPF routing process.

Configuration Examples The following example displays the output of the **show ip ospf** command.

```
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
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, 10 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group:240 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
Number 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
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled, Stability Interval expired in 00:00:03
```

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF
Conforms to RFC2328	Same as the RFC2328
RFC1583Compatibilit flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database

Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.
BFD enabled	Enables BFD for OSPF.

This series does not support BFD and VRF.

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

2.52 show ip ospf border-routers

Use this command to display the OSPF internal routing table on the ABR/ASBR.

show ip ospf [*process-id***] border-routers**

Parameter Description	Parameter	Description
	process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the show ip route command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.

Configuration Examples The following example displays the output of the **show ip ospf border-mrouters** command.

```
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, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
The following table describes fields in the output.
```

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Displays the OSPF ID of the border device.
[2]	Displays the cost to the border device.
via 10.0.0.1	Displays the next-hop gateway to the border device.
FastEthernet 0/1	Displays the interface to the border device.
ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Displays the area that learns the route.
select	Indicates the currently selected optimal path when there are multiple

	paths to the ASBR.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.53 show ip ospf database

Use this command to display the OSPF link state database information. Use the **no** form of this command to restore the default setting. Different formats of the command will display different LSA information.

show ip ospf [*process-id* [*area-id* | *ip-address*]] **database** [{ **asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary** }] [{ **adv-router** *ip-address* **| self-originate } |** *link-state-id* **| brief**] [**database-summary | max-age | detail**]

Parameter Description

Parameter	Description
area-id	(Optional) Displays the area ID.
adv-device	(Optional) Displays the LSA information generated by the specified advertising device.
link-state-id	(Optional) Displays the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Displays the LSA information generated by the device itself.
Max-age	(Optional) Displays the LSAs aged.
router	(Optional) Displays the OSPF device LSA information.
network	(Optional) Displays the OSPF network LSA information.
summary	(Optional) Displays the OSPF summary LSA information.
asbr-summary	(Optional) Displays the ASBR summary LSA information.
external	(Optional) Displays the OSPF external LSA information.
nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
opaque-area	(Optional) Displays type 10 LSAs.
opaque-as	(Optional) Displays type 11 LSAs.
opaque-link	(Optional) Displays type 9 LSAs.
database-summary	(Optional) Displays the statistics of LSAs of the link state database.
detail	Displays detailed information of LSAs of the OSPF.
brief	Displays the brief information of the LSAs of the specified type.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration Examples The following example displays the output of the **show ip ospf database** command.

```
Hostname# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID        ADV Device     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 Device     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 Device     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
Device Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     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 Device     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 Device     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 Device     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
```

The following table describes the fields in the output of the **show ip ospf database** command.

Field	Description
OSPF Device with ID	Displays the Router ID.
Device Link States	Displays the device LSA information.
Net Link States	Displays the network LSA information.
Summary Net Link States	Displays the summary network LSA information.
NSSA-external Link	Displays the type 7 autonomous external LSA information.

States	
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.

```
Hostname# show ip ospf database asbr-summary
     OSPF Device 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 Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
     TOS: 0  Metric: 1
```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.

Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database external** command.

```
Hostname# show ip ospf database external
     OSPF Device 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 Device: 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
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.

Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```
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
```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.
Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```
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
```

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.

Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only
TOS 0 Metrics	TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
Hostname# show ip ospf database summary
     OSPF Device 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 Device: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
     TOS: 0  Metric: 11
```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.

Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```
Hostname# show ip ospf database nssa-external
     OSPF Device 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 Device: 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
```

The following table describes the fields in the output of the **show ip ospf database nssa-external** command.

Field	Description
OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.

LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database external** command:

```
Hostname# show ip ospf database external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
         AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 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
```

The following table describes the fields in the output of the **show ip ospf database external**

command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary** command:

```
Hostname# show ip ospf database database-summary
OSPF process 1:
Device 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
```

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area
NSSA-external Link	Number of NSSA LSAs in the area

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.54 show ip ospf interface

Use this command to display the OSPF-associated interface information.

show ip ospf [*process-id* **] interface [** *interface-type interface-number* **| brief]**

Parameter Description

Parameter	Description
process-id	OSPF process ID
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface
brief	Displays the summary of the interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF information on the interface.

Configuration Examples The following example displays the output of the **show ip ospf interface fastEthernet** *0/1* command:

```
Hostname# show ip ospf interface fastEthernet0/1
FastEthernet 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
```

The following table describes the fields in the output of the **show ip ospf interface serial***1/0* command.

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface

Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.55 show ip ospf neighbor

Use this command to display the OSPF neighbor list.

show ip ospf [*process-id*] **neighbor[statistics** | { [*interface-type interface-number*] | [*neighbor-id*] | [**detail**] }]

Parameter Description

Parameter	Description
process-id	Displays ID of the process.
detail	(Optional) Displays the neighbor details.
interface-type interface-number	(Optional) Displays the neighbor information of the specified interface
neighbor-id	(Optional) Displays the information of the specified neighbor
statistics	(Optional) Displays the neighbor statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays neighbor information usually used to check whether the OSPF is running normally.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.56 show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [**count |** *ip-address mask*]

Parameter Description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes
ip-address mask	Statistics of routes which have a specified prefix and mask.

Defaults N/A

Command Mode Privileged mode

Usage Guide This command displays the OSPF routing information. The count option displays the OSPF routing statistics.

Configuration Examples The following example displays the output of the **show ip ospf route** command.

```
OSPF process 1:
Codes: C - connected, D - Discard , 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, FastEthernet 0/1
C  192.88.88.0/24 [1] is directly connected,FastEthernet 0/1,Area 0.0.0.1
```

The following table describes the fields in the output of the **show ip ospf route** command.

Field	Description
codes	Route type and corresponding abbreviation and description
100.0.0.0/24	Route prefix

[1]	Route cost
via	Route next hop and interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.57 show ip ospf spf

Use this command to display the routing count in the OSPF area.

show ip ospf [*process-id*] **spf**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration Examples The following example displays the output of the **show ip ospf [***process-id***] spf** command:

```
Hostname# show ip ospf 1 spf

OSPF process 1:
Area_id     30min_counts   Total_counts
0               32             1235
1               6               356
```

The following table describes the fields in the output of the **show ip ospf [***process-id***] spf** command.

Field	Description
Area_id	OSPF area ID
30min_counts	OSPF routing counts within the latest 30 minutes
Total_counts	Total counts of the OSPF routing till now

Related Commands

Command	Description

show ip ospf	Displays the OSPF summary.

Platform Description N/A

2.58 show ip ospf summary-address

Use this command to display the converged route of all redistributed routes.

show ip ospf [*process-id***] summary-address**

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.

Configuration Examples The following example displays the output of the **show ip ospf summary-address** command:

```
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
```

Field	Description
Summary Address	IP address to be aggregated
Summary Mask	Mask to be aggregated
Advertise	Whether to advertise the aggregated route
Status	Whether the aggregation range takes effect
Aggregated subnets	Number of external routes included in the aggregation range

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.59 show ip ospf virtual-link

Use this command to display the OSPF virtual link information.

show ip ospf [*process-id*] **virtual-link** [*ip-address*]

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
ip-address	Associated ID of a virtual link neighbor

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If no virtual link is configured, the command displays the neighbor status and other related information. The show ip ospf neighbor command does not display the neighbor of the virtual link.

Configuration Examples The following is the output of the **show ip ospf virtual-links** command:

```
Hostname# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 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
```

The following table describes the fields in the output.

Field	Description
Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
Virtual Link State	Displays the virtual link state.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Displays the transmit delay of the virtual link.
State	Interface state
Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface

Adjacency State	Neighbor state, where FULL means the stable state

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.60 summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to restore the remove the aggregate route.

summary-address *ip-address net-mask* [**not-advertise** | **tag** *value* | **cost** *cost*]

no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

Parameter Description

Parameter	Description
ip address	IP address of the aggregate route
net-mask	Network mask of the aggregate route
not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
tag *value*	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.
cost *cost*	Cost value of the aggregate route. The range is from 0 to 16,777,214.

Defaults No aggregate route is configured by default.

Command Mode Routing process configuration mode

Usage Guide When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly.

Unlike the **area range** command, the area range command aggregates inter-OSPF-area routes, while the summary-address command aggregates external routes of the OSPF routing domain.

For the NSSA, the **summary-address** command is valid only on the NSSA ABR now, and aggregates only redistributed routes.

Configuration Examples The following example generates an external aggregate route 100.100.0.0/16.

```
Hostname(config)# router ospf20
Hostname(config-router)# summary-address100.100.0.0 255.255.0.0
```

```
Hostname(config-router)# redistribute static subnets
Hostname(config-router)# network200.2.2.0 0.0.0.255 area 1
Hostname(config-router)# network172.16.24.0 0.0.0.255area 0
Hostname(config-router)# area1nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

2.61 timers lsa arrival

Use this command to configure the time delay for the same LSA received. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
arrival-time	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.

Defaults The default is 1000.

Command Mode Routing process configuration mode

Usage Guide No action is done when the same LSA is received within the specified time.

Configuration Examples The following example configures the time delay for the same LSA as 2seconds.

```
Hostname(config)# routerospf1
Hostname(config-router)# timers arrival-time 2000
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.62 timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to1800 in the unit of seconds.

Defaults The default is 30.

Command Mode Routing process configuration mode

Usage Guide Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches.

You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.

Configuration Examples The following example configures the pacing time as 120 seconds.

```
Hostname(config)# deviceospf 20
Hostname(config-router)# timers paing lsa-group 120
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.63 timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
transmit-time	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
transmit-count	Configures the number of LS-UPD packets per group. The range is from 1 to 200.

Defaults The default configurations are as follows:
Transmit-time: 40 milliseconds.
Transmit-count: 1

Command Mode Routing process configuration mode

Usage Guide If there are a large number of LSAs and the load on the system is heavy, you can properly use the **transmit-time** and **transmit-count** to inhibit the flooding LS-UPD packet number in the network.
If the CPU and network bandwidth loads are not too much, reduce **transimi-time** and increase **transimit-count** to quicken the environment convergence.

Configuration Examples The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.

```
Hostname(config)# routerospf1
Hostname(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF process information, including the router ID.

Platform Description N/A

2.64 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the **no** form of this command to restore the default setting.
timers spf *spf-delay spf-holdtime*
no timers spf

Parameter Description

Parameter	Description

spf-delay	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647.After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647.When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Defaults The system supports the timers throttle spf command. By default, the timers spf command takes no effect. Spf-delay depends on the default configuration of the timers throttle spf command.

Command Mode Routing process configuration mode

Usage Guide Smaller values of *spf-delay* and *spf-holdtime* mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.

⚠ The configurations of the **timers spf command** and the timers throttle spf command may overwrite each other.

Configuration Examples The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
Hostname(config)# deviceospf20
Hostname(config-router)# timersspf 3 9
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf.
timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the timers spf command because it is more powerful.

Platform Description N/A

2.65 timers throttle lsa all

Use this command to configure the exponential back off algorithm for the LSA. Use the **no** form of this command to restore the default setting.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	Description
delay-time	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
hold-time	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from1 to 600000.
max-wait-time	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from1 to 600000

Defaults

The default configurations are as follows:
Delay-time: 0 millisecond,
Hold-time: 5000 milliseconds,
Max-wait-time: 5000 milliseconds.

Command Mode

Routing process configuration mode

Usage Guide

If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.

⚠ The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time cannot be smaller than that of hold-time.

Configuration Examples

The following example configures the first delay as 10ms, hold-time as 1second and the longest delay as 5seconds.

```
Hostname(config)# routerospf1
Hostname(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf

Platform Description

N/A

2.66 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting.
timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
ia-delay	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults The default values are as follows:
ia-delay: 0,
ase-delay: 0,

Command Mode Routing process configuration mode

Usage Guide The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples The following example sets the .delay time of the inter-area route calculation to one second.

```
Hostname(config)# router ospf 1
Hostname(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.67 timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the **no** form of this command to restore the default setting.
timers throttle spf *spf-delay spf-holdtime spf-max-waittime*
no timers throttle spf

Parameter Description

Parameter	Description
spf-delay	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds in the range from1 to 600,000.
spf-max-waittime	Defines the maximum interval between two SPF calculations, in milliseconds in the range from1 to 60,0000.

Defaults

The default configurations are as follows:
spf-delay: 1000ms;
spf-holdtime: 5000ms;
spf-max-waittime: 10000ms.

Command Mode

Routing process configuration mode

Usage Guide

The spf-delay parameter indicates the delay time of the topology change to the SPF calculation.
The spf-holdtime parameter indicates the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to spf-max-waittime. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will restart from spf-holdtime.
Smaller spf-delay and spf-holdtime values can make the topology converge faster. A greater spf-max-waittime value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology.
Compared with the timers spf command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the timers throttle spf command is recommended.

The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value ofspf-holdtime will be set to be equal to the value of spf-delay;
The value of spf-max-waitime cannot be smaller than the value of spf-holdtime, or the value of spf-max-waittime will be set to be equal to the value of spf-holdtime automatically;
The configurations of the timers spf command and the timers throttle spf command may overwrite each other.
If both the timers spf command and the timers throttle spf command are not configured, the default value of the timers throttle spf command is used.

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds,

89 seconds, 179 seconds, 179+90seconds…

```
Hostname(config)# routerospf20
Hostname(config-router)# timersspf 5 1000 90000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of OSPF
timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than RGOS 10.4. It is recommended to replace the timers spf command with the timers throttle spf command.

Platform Description N/A

2.68 two-way-maintain

Use this command to enable the OSPF two-way-maintain function. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.

Configuration Examples The following example disables the OSPF two-way-maintain function.

```
Hostname(config)# routerospf1
Hostname(config-router)# notwo-way-maintain
```

Related

Command	Description

Commands

show ip ospf	Displays the configuration information of the OSPF

Platform Description N/A

3 RIPng Commands

3.1 clear ipv6 rip

Use this command to clear the RIPng routes.

clear ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults None

Command mode Privileged EXEC mode

Usage Guide Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

Configuration Examples The following example clears the RIPng routes:

```
Hostname# clear ipv6 rip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.2 default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

Defaults The default value is 1.

Command mode Routing process configuration mode.

Usage Guide This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Configuration Examples The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
Hostname(config-router)# default-metric 3
Hostname(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the route from one route domain to another route domain.

Platform Description N/A

3.3 distance

Use this command to set the administrative distance of RIPng. Use the **no** form of this command to restore the default value.

distance *distance*

no distance

Parameter Description

Parameter	Description
distance	Sets the RIPng administrative distance. The range is from 1 to 254.

Defaults The default distance is 120

Command mode Routing process configuration mode.

Usage Guide N/A

Configuration The following example shows how to set the RIPng administrative distance as 160:

Examples

```
Hostname(config)# ipv6 router rip
Hostname(config-router)# distance 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 distribute-list

Use this command to filter the in/out route in the prefix list. Use the **no** form of this command to remove route filtering.

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

Parameter Description

Parameter	Description
prefix-list *prefix-list-name*	Name of the prefix list which is used to filter the route.
in | **out**	Filters the in or out route in the distribute list.
interface-type interface-name	(Optional) Applies the distribute list to the specified interface.

Defaults By default, no distribute list is defined.

Command mode Routing process configuration mode.

Usage Guide This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Configuration Examples The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list** *allowpre* prefix list range can be received)

```
Hostname(config)# ipv6 router rip
Hostname(config-router)# distribute-list prefix-list allowpre in eth0
```

Related Commands

Command	Description
redistribute	Sets route redistribution.

Platform Description N/A

3.5 graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.
graceful-restart [**grace-period** *grace-period*]

Use the **no** form of this command restore the default configurations.
no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	Displays the configured grace period.
grace-period	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.

Defaults The GR function is enabled by default.

Command Mode Routing process configuration mode

Default Level 14

Usage Guide The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.
The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.
The **graceful-restart grace-period** command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:
If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the **timers** command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.
When GR is performed for the RIPng process, ensure that the network environment is stable.

Configuration Examples The following example enables the GR function for the RIPng process and configures the GR period.

```
Hostname(config)# ipv6 router rip
```

```
Hostname(config-router)# graceful-restart grace-period 90
```

Verification Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

Prompts N/A

Common Errors N/A

Platform Description N/A

3.6 ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

ipv6 rip default-information { **only** | **originate**} [**metric** *metric-value*]

no ipv6 rip default-information

Parameter Description

Parameter	Description
only	Advertises the IPv6 default route only.
originate	Advertises both of the IPv6 default route and other routes.
metric *metric-value*	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

Defaults By default, no default route is configured.

Command mode Interface configuration mode

Usage Guide With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Configuration Examples The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

```
Hostname(config)# interface ethernet 0/0
Hostname(config-if)# ipv6 rip default-information only
```

Related Commands

Command	Description

show ipv6 rip	Displays the RIPng process and statistics.
show ipv6 rip database	Displays the RIPng route.

Platform Description N/A

3.7 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

ipv6 rip enable

no ipv6 rip enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults It is disabled by default.

Command mode Interface configuration mode.

Usage Guide This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Configuration Examples The following example shows how to enable the RIPng on the interface 0/0:

```
Hostname(config)# interface ethernet 0/0
Hostname(config-if)# ipv6 rip enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

ipv6 rip metric-offset *value*

no ipv6 rip metric-offset

Parameter Description

Parameter	Description
value	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults The default value is 1.

Command mode Interface configuration mode.

Usage Guide Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

Configuration Examples The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:

```
Hostname(config)# interface ethernet 0/1
Hostname(config-if)# ipv6 rip metric-offset 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use the **no** form of this command to remove the RIPng process.

ipv6 router rip

no ipv6 router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults No RIPng process is configured by default.

Command mode Global configuration mode.

Usage Guide N/A.

Configuration Examples The following example shows how to create the RIPng process and enter routing process configuration mode:

```
Hostname(config)# ipv6 router rip
```

Related Commands

Command	Description
ipv6 rip enable	Enables the RIPng on the specified interface.

Platform Description N/A

3.10 passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command to enable the interface to send update packets.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Enables the passive mode on all interfaces.
interface-type interface-num	Interface type and interface number.

Defaults No passive interface is configured by default.

Command mode Routing process configuration mode.

Usage Guide You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then ,use the **no passive-interface** *interface-type interface-num* command to remove the specified interface from the passive mode.

Configuration Examples The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode:

```
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface ethernet 0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this command to remove the redistribution configuration.

redistribute { **connected** | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

no redistribute { **connected** | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

Parameter Description

Parameter	Description
connected	Redistributes the connected routes to RIPng.
static	Redistributes the static routes to RIPng.
metric *metric-value*	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map *route-map-name*	(Optional) Sets the redistribution route filtering.

Defaults

By default, the routes of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1;

By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to redistribute the external routes to RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

Configuration Examples

The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

```
Hostname(config)# ipv6 router rip
Hostname(config-router)# redistribute static route-map
mymap metric 8
```

Related Commands

Command	Description
default-metric	Defines the default RIPng metric value when redistributing other routing protocols.
distribute-list	Filters the RIPng routing update packets.

Platform Description

N/A

3.12 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

show ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
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
Default distance 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
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.

Platform Description N/A

3.13 show ipv6 rip database

Use this command to display the RIPng route entries.

show ipv6 rip database

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
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/::
```

This series does not support BGP. The configuration example is only for reference.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.14 split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the **no** form of this command to disable this function.

split-horizon [**poisoned-reverse**]

no split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.

Defaults RIPng split horizon is enabled by default.

Command mode Routing process configuration mode.

Usage Guide In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

Configuration Examples The following example shows how to disable the RIPng horizontal split:

```
Hostname(config)# ipv6 router rip
Hostname(config-router)# no split-horizon
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 timers

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore the default settings.

timers *update invalid flush*

no timers

Parameter Description

Parameter	Description
update	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
invalid	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
flush	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Defaults The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

Command mode Routing process configuration mode.

Usage Guide Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.
Use the **show ipv6 rip** command to view the current RIPng time parameter setting.
In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Configuration Examples The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
Hostname(config)# ipv6 router rip
Hostname(config-router)# timers 10 30 90
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and the statistical information of the RIPng process.
show ipv6 rip database	Displays the RIPng routes.

Platform N/A

Description

4 NSM Commands

4.1 clear ip route

Use this command to clear the route cache.

clear ip route { ***** **|** *network* [*netmask*] | }

Parameter Description

Parameter	Description
*	Clears all route cache.
network	Specifies the route cache of the network or subnet.
netmask	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match *network* with the route. The cache of the longest match is cleared.

Command Mode Privileged EXEC mode

Usage Guide Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. Please note that clearing all route cache leads to temporary network disconnection.

Examples The following example clears the cache of the route which is the longest match with IP address 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.2 ip default-gateway

Use this command to configure the default gateway IP address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

ip default-gateway *ip-address*

no ip default-gateway

default ip default-gateway

Parameter Description

Parameter	Description
ip-address	IPv4 address of the default gateway

Defaults No gateway IP address is configured by default.

Command Mode Global configuration mode

Usage Guide When the device does not know the destination address of a packet, the device will forward the packet to the default gateway.

Examples The following example sets the IP address of default gateway to 192.168.1.1.

```
ip default-gateway 192.168.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

4.3 ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

ip default-network *network*

no ip default-network *network*

default ip default-network *network*

Parameter Description

Parameter	Description
network	Default network

Defaults The default is 0.0.0.0/0.

Command Mode Global configuration mode

Usage Guide The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.
The default network always starts with an asterisk (“*”), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

Examples The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
```

```
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

Related Commands

Command	Description
show ip route	Displays the routing table.

4.4 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.

ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent |** [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]

no ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

default ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

Parameter Description

Parameter	Description
network	Network address of the destination
net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The administrative distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent route ID
weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
description *description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.

Defaults No static route is configured by default.

Command Mode Global configuration mode

Usage Guide The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over to the static route when the route running OSPF fails.

The default weight of the static route is 1. To view the static route of non-default weight, execute the **show ip route weight** command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

Association between a static route and a track object can be specified. When association between a static route and a specified track object is configured and the advertised track object status is inactive, the static route does not take effect. If the advertised track object status is active, the static route takes effect based on another status. With association between a static route and a track object, the third-party status concerned by the track object is mainly used to determine whether the static route takes effect. Association between a static route and a track object cannot be used for routes with the permanent attribute.

Association between a static route and an ARP object can be specified. When association between a static route and 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. Association between a static route and an ARP object cannot be used for routes with the permanent attribute.

Association between a static route and a track object cannot be used together with association between a static route and an ARP object.

Examples

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures data flows to be sent through fastehternet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

Related Commands N/A

4.5 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this

command to disable this function.
ip routing
no ip routing
default ip routing

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide
IP routing is not necessary when the switch serves as bridge or VoIP gateway.
When a device functions only as a bridge or VoIP gateway, the IP routing function of the system software is not required. In this case, the IP routing function of the system software 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 IP routing.

```
Hostname(config)# no ip routing
```

Related Commands N/A

Platform Description N/A

4.6 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.
ip static route-limit *number*
no ip static route-limit *number*
default ip static route-limit

Parameter Description

Parameter	Description
number	Upper threshold of static routes in the range from 1 to 10000

Defaults The default is 1024.

Command Mode Global configuration mode

Usage Guide The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

Examples The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
ip static route-limit 900
```

Related Commands N/A

Platform Description N/A

4.7 ipv6 default-gateway

Use this command to configure the default gateway IPv6 address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

default ipv6 default-gateway

Parameter Description

Parameter	Description
ipv6-address	Sets the default gateway IPv6 address.

Defaults No gateway IPv6 address is configured by default.

Command Mode Global configuration mode

Usage Guide When the device does not know the destination address of a packet, the device will forward the packet to the default gateway. Use the command **show ipv6 redirects to** display default gateway configuration.

Examples The following example sets the default gateway IPv6 address to 10::1.

```
Hostname(config)# ipv6 default-gateway 10::1
```

Platform Description N/A

4.8 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.

ipv6 route *ipv6-prefix* / *prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

no ipv6 route*ipv6-prefix* / *prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*]

default ipv6 route *ipv6-prefix* / *prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*]

Parameter Description

Parameter	Description
ipv6-prefix	IPv6 prefix. It must comply with RFC4291.
prefix-length	Mask length of the destination
ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The administrative distance of the static route. The default is 1.
tag	(Optional) The tag value of the static route. The default is 0.
weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. 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 weight is 1 by default.
description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.

Defaults No IPv6 static route is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Examples

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Related Commands

Command	Description
show ipv6 route	Displays IPv6 routing table.

Platform Description N/A

4.9 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

Ipv6 static route-limit *number*

no ipv6 static route-limit *number*

default ipv6 static route-limit

Parameter Description

Parameter	Description
number	Upper threshold of static routes in the range from 1 to 10000.

Defaults The default is 1000.

Command Mode Global configuration mode

Usage Guide The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

Examples The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.

```
Hostname (config)# ipv6 static route-limit 900
Hostname(config)# no ipv6 static route-limit
```

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Platform Description N/A

4.10 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the system. Use the **no** or **default** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

default ipv6 unicast-routing

Parameter Description N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

Examples The following example disables the IPv6 route function of the system.

```
Hostname# no ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 route	Configure the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Platform Description N/A

4.11 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

maximum-paths *number*

no maximum-paths *number*

default maximum-paths

Parameter Description

Parameter	Description
number	Number of equivalent routes, which is 1.

Defaults The default value varies with the device model.

Command Mode Global configuration mode

Usage Guide The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent 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 static routes. You can run the **show running config** command to query the number of configured static routes. This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value.

Examples The following example sets the number of equivalent routes to 1 and then restores the default setting.

```
Hostname(config)# maximum-paths 1
Hostname(config)# no maximum-paths
```

4.12 show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the default gateway IP address. This command is supported on 2-layer devices or 3-layer devices with the **no ip routing** command executed.

Examples The following example displays the default gateway.

```
Hostname# show ip redirects
Default Gateway: 192.168.195.1
```

Field	Description
Default Gateway	IP address of the default gateway.

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

4.13 show ip route

Use the commands to display the configuration of the IP routing table.

show ip route *network* [*mask* [**longer-prefix**]] | **count** | *protocol* [*process-id*] | **weight**]]

show ip route [**normal** | **ecmp**] [*network* [*mask*]]

Parameter Description

Parameter	Description
network	(Optional) Displays the route information to the network.
mask	(Optional)Displays the route information to the network of this mask.
longer-prefix	(optional) Displays the routes that match the specified prefix.
count	(Optional)Displays the number of existent routes. (for the ECMP/WCMP route, displays one route)
protocol	(Optional) Displays the route information of specific protocol.
process-id	(Optional) Routing protocol process ID.
weight	(Optional) Displays the route information of non default weight.
normal	Displays normal routes and not equivalent routes or fast reroutes.
ecmp	Displays only equivalent routes.

Defaults All routes are displayed by default.

Command Mode Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

Usage Guide This command can display route information flexibly.
This command shows all routes. To show different attributes of routes, specify normal | ecmp.

Examples The following example displays the configuration of the IP routing table.

```
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, * - 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.
```

```
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
```

```
Hostname# show ip route count
--------- route info ----------
the num of active route: 9
```

```
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
```

```
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
```

```
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
```

This series does not support ISIS or BGP. The configuration example is only for reference.

4.14 show ip route summary

Use this command to display the statistical information about one routing table.

show ip route summary

Use this command to display the statistical information about all routing tables.

show ip route summary all

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage guideline N/A

The following example displays the statistics of the global routing table.

```
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
                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
```

Examples

The following example displays the statistics of all routing tables.

```
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
                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
                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
```

This series does not support ISIS or BGP. The configuration example is only for reference.

Field	Description
NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

4.15 show ipv6 redirects

Use this command to display the IPv6 default gateway IP address.

show ipv6 redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Examples

The following example displays the default gateway IPv6 address.

```
Hostname# show ipv6 redirects
Default Gateway: 10::1
```

Field	Description
Default Gateway	IPv6 address of the default gateway

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.16 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

show ipv6 route [[*ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *protocol* | **weight**]]

Parameter Description

Parameter	Description
ipv6-prefix/*prefix-length*	(Optional) Specifies a prefix for route's IPv6 address.
longer-prefixes	(Optional) Displays the route with an IPv6 address prefix mostly matched.
protocol	(Optional) Displays the route information of specific protocol.
process-id	(Optional) Specifies a route process ID.
weight	(Optional) Displays the non-default-weight routes only.

Defaults All routes are displayed by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to display route information.

Examples N/A

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.

Platform

Description N/A

4.17 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table of a specified VRF.

show ipv6 route summary

Use this command to display statistics of all IPv6 routing tables.

show ipv6 route summary all

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Examples

The following example displays statistics of IPv6 routing table of the global VRF.

```
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
PIP           0
OSPF          0
BGP           0
------------------------
Total          5
```

The following example displays t statistics of all IPv6 routing tables.

```
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
PIP           0
OSPF          0
BGP           0
------------------------
Total          5
```

This series does not support ISIS or BGP. The configuration example is only for reference.

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Multicast Commands

1. IPv4 Multicast Routing Commands
2. IGMP Snooping Commands

1 IPv4 Multicast Routing Commands

1.1 ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** form of this command removes the setting.

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

Parameter Description

Parameter	Description
source-address	Source IP address
group-address	IP address of the multicast group
interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default Disabled

Command Mode Global configuration mode

Usage Guide

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.

Examples

The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
Hostname(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6
Hostname(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2
```

1.2 msf immediately-install

Use this command to enable immediate delivery of IPv4 multicast Layer 2 entries to the forwarding plane. Use the **no** or **default** form of this command to disable this function.

msf immediately-install

no msf immediately-install

default msf immediately-install

Parameter Description	Parameter	Description
	N/A	N/A

Default Disabled.

Command Mode Global configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples

The following example enables immediate delivery of IPv4 multicast Layer 2 entries to the forwarding plane.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# msf immediately-install
```

Verification Run the **show running-config** command to check whether the function of immediate delivery of IPv4 multicast Layer 2 entries to the forwarding plane is enabled.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.3 msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism. Use the **no** or **default** form of this command to disable the overflow overriding mechanism.

msf ipmc-overflow override

no msf ipmc-overflow override

default msf ipmc-overflow override

Parameter Description	Parameter	Description
	-	-

Default Disabled.

Command Mode Global configuration mode.

Usage Guide N/A

Examples The following example enables the overflow overriding mechanism.

```
Hostname (config)# msf ipmc-overflow override
Hostname (config)#
```

1.4 msf nsf

Use this command to configure the parameter for the continuous multicast forwarding. Use the **no** or **default** form of this command to restore the default setting.

msf nsf {{**convergence-time** *time*} | {**leak** *interval*} }

no msf nsf {**convergence-time** | **leak**}

default msf nsf { **convergence-time** | **leak** }

Parameter Description

Parameter	Description
convergence-time *ttl-value*	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
leak *interval*	Packet multicast leak time, in the valid range of 0-3600s

Default convergence-time *time* :140s;
leak interval: 150s

Command Mode Global configuration mode.

Usage Guide N/A

Examples The following example sets the maximum time for the protocol convergence.

```
Hostname (config)# msf nsf convergence-time 300
Hostname (config)#
```

The following example sets the packets leak time:

```
Hostname(config)# msf nsf leak 200
Hostname(config)#
```

1.5 show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

show msf msc [*soure-address*] [*group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
source-address	Specified source IP address of the multi-layer multicast forwarding table.
group-address	Specified group address of the multi-layer multicast forwarding table.
vlan-id	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. 4096 indicates a routed port.

Default

Command Mode

Privileged EXEC mode/Global configuration mode/Interface EXEC mode

Usage Guide

The three parameters in this command are optional.

If no source address and group address are specified, all mfc entries are displayed.

- If only the source address is specified as s1, all msc entries with source address 1 are displayed.
- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.
- Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

Examples

The following example shows the IPv4 layer-3 multicast forwarding entries with source IP address 192.168.195.25:

```
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
```

The fields in the execution of the **show mrf mfc** command are described in the following table.

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.

OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

1.6 show msf nsf

Use this command to show the configuration of continuous multicast forwarding.

show msf nsf

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/Global configuration mode/Interface EXEC mode

Examples

The following example shows the configuration of continuous multicast forwarding.

```
Hostname# show msf nsf
Multicast HA Parameters
-------------------------------------------------+------+
protocol convergence timeout 120 secs
flow leak interval 20 secs
Hostname#
```

Related Commands

Command	Description
msf nsf	Configure the multicast NSF parameter.

2 IGMP Snooping Commands

2.1 clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

clear ip igmp snooping gda-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

Configuration Examples The following example clears the Group Destination Address (GDA) table.

```
Hostname# clear ip igmp snooping gda-table
```

Platform Description N/A

2.2 clear ip igmp snooping statistics

Use this command to clear IGMP Snooping statistics.

clear ip igmp snooping statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the IGMP Snooping statistics, which can be displayed by using the **show ip igmp snooping statistics** command.

Configuration Examples The following example clears the IGMP Snooping statistics.

```
Hostname# clear ip igmp snooping statistics
```

Platform Description N/A

2.3 deny

Use this command to deny the forwarding of the multicast streams in the range specified by the profile.

deny

Parameter Description

Parameter	Description
N/A	N/A

Defaults The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode Profile configuration mode

Usage Guide First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Configuration Examples The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244.

```
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# deny
```

Platform Description N/A

2.4 ip igmp profile

Use this command to create a profile and enter the IGMP profile configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

default ip igmp profile *profile-number*

Parameter

Parameter	Description

Description

profile-number	Profile number, in the range from 1 to 1024

Defaults No profile is created by default.

Command Mode Global configuration mode

Usage Guide The profile is a filter to permit/deny specified groups in the following steps:

- Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
- Use the **range** command to define a profile range.
- Use the **permit** command to permit this profile in the filtering, or use the **deny** command to deny this profile in the filtering.
- If the **deny** command is used without any profile specified, all profiles in the profile are permitted.
- If the **permit** command is used without any profile specified, all profiles in the profile are denied.

Configuration Examples The following example creates and permits profile 1 with addresses from 224.2.2.2 to 224.2.2.244.

```
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# permit
```

Platform Description N/A

2.5 ip igmp snooping

Use this command to enable IGMP snooping and enter the IVGL mode.

ip igmp snooping ivgl

Use this command to enable IGMP snooping and enter the SVGL mode.

ip igmp snooping svgl

Use this command to enable IGMP snooping and enter the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

Use the **no** or **default** command to restore the default setting.

no ip igmp snooping

default ip igmp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults IGMP Snooping is disabled by default.

Command Global configuration mode

Mode

Usage Guide

- **IVGL (Independent VLAN Group Learning):** In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.
- **SVGL (Shared VLAN Group Learning):** In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicast flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3:
- **IVGL-SVGL mode:** also known as promiscuous mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.

SVGL mode and IVGL-SVGL mode conflict with the IP multicast function.

PIM Snooping must depend on either IVGL or IVGL-SVGL mode of IGMP Snooping. Use **no ip igmp snooping** command to disable IGMP Snooping after PIM Snooping is disabled.

Configuration Examples

The following example enables IGMP Snooping and enters the IVGL mode.

```
Hostname(config)# ip igmp snooping ivgl
```

The following example enables IGMP Snooping and enters the SVGL mode.

```
Hostname(config)# ip igmp snooping svgl
Hostname(config)# ip igmp snooping svgl profile 1
```

The following example enables IGMP Snooping and enters the IVGL-SVGL mode.

```
Hostname(config)# ip igmp snooping ivgl-svgl
Hostname(config)# ip igmp snooping svgl profile 1
```

Platform Description

N/A

2.6 ip igmp snooping dyn-mr-aging-time

Use this command to set the aging time of a dynamic routing interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping dyn-mr-aging-time *seconds*

no ip igmp snooping dyn-mr-aging-time

default ip igmp snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
seconds	Aging time from 1 to 3,600 in the unit of seconds

Defaults The default is 300 seconds.

Command Mode Global configuration mode

Usage Guide If a dynamic routing interface does not receive IGMP query packets or PIM hello packets before aged, this interface will be deleted.
When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

Configuration Examples The following example sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Hostname(config)# ip igmp snooping dyn-mr-aging-time 100
```

Platform Description N/A

2.7 ip igmp snooping fast-leave enable

Use this command to enable the fast leave function.
Use the **no** or **default** form of this command to restore the default setting.
ip igmp snooping fast-leave enable
no ip igmp snooping fast-leave enable
default ip igmp snooping fast-leave enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.
Subsequently, when the system receives a specific group query packet, the system does not forward it

to the corresponding interface. Leave packets include IGMPv2 leave packets and IGMPv3 report packets of the include type without source addresses. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

Configuration Examples The following example enables the fast leave function.

```
Hostname(config)# ip igmp snooping fast-leave
```

Platform Description N/A

2.8 ip igmp snooping filter

Use this command to specify the profile for ports.
Use the **no** or **default** form of this command to restore the default setting.
ip igmp snooping filter *profile-number*
no ip igmp snooping filter *profile-number*
default ip igmp snooping filter

Use this command to specify the profile for VLANs.
Use the **no** or **default** form of this command to restore the default setting.
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

Parameter	Description
profile-number	Profile number from 1 to 1024

Defaults This function is disabled by default.

Command Mode Global configuration mode/Interface configuration mode

Usage Guide A specific profile must be created before association.

Configuration Examples The following example specifies profile 1 for interface fastEthernet 0/1.

```
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip igmp snooping filter 1
```

Platform Description N/A

2.9 ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping host-aging-time *seconds*

no ip igmp snooping host-aging-time

default ip igmp snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Aging time. The unit is second. The value ranges from 1 to 65,535.

Defaults The default is 260 seconds.

Command Mode Global configuration mode

Usage Guide The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.

When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

Configuration Examples The following example sets the aging time to 30 seconds.

```
Hostname(config)# ip igmp snooping host-aging-time 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 ip igmp snooping ivgl

Use this command to enable IGMP snooping globally and set it to IVGL mode.

ip igmp snooping ivgl

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

no ip igmp snooping ivgl

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

default ip igmp snooping ivgl

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Disabled.

Command Mode Global configuration mode

Default Level 14

Usage Guide In the IVGL mode, multicast data in each VLAN is independent. 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 can forwards the data only to member ports in the same VLAN.

Configuration Examples The following example enables IGMP snooping globally and sets it to the IVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping ivgl
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

2.11 ip igmp snooping ivgl

Use this command to enable IGMP snooping globally and set it to the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

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

no ip igmp snooping ivgl-svgl

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

default ip igmp snooping ivgl-svgl

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Disabled.

Command Mode Global configuration mode

Default Level 14

Usage Guide In the IVGL-SVGL mode, the IVGL and SVGL mode coexist. A profile must be used to define an address 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.

Configuration Examples The following example enables IGMP snooping globally and sets it to the IVGL-SVGL mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip igmp snooping ivgl-svgl
```

Verification N/A

Prompt Messages N/A

Common Errors

Platform Description N/A

2.12 ip igmp snooping l2-entry-limit

Use this command to set the maximum number of multicast groups.
Use the **no** or **default** form of this command to restore the default setting.
ip igmp snooping l2-entry-limit *number*
no ip igmp snooping l2-entry-limit
default ip igmp snooping l2-entry-limit

Parameter Description

Parameter	Description
number	Number of multicast groups. The value ranges from 0 to 65,536.

Defaults The default is 65,536.

Command Mode Global configuration mode

Usage Guide The maximum number of multicast groups includes the multicast groups in all ports of all VLANs (including dynamic and static multicast groups). When the number of multicast groups reaches the limit, learning new group records and configuring new static multicast group ports are not allowed.

Configuration Examples The following example sets the maximum number of multicast groups to 2000.

```
Hostname(config)# ip igmp snooping l2-entry-limit 2000
```

Related Commands

Command	Description

show ip igmp snooping	Displays the maximum number of multicast groups.

Platform Description N/A

2.13 ip igmp snooping max-groups

Use this command to configure the maximum number of groups that can be added dynamically to this interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

default ip igmp snooping max-groups

Parameter Description

Parameter	Description
number	The maximum group number from 0 to 1,024

Defaults No maximum group number is configured by default.

Command Mode Interface configuration mode

Usage Guide If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

Configuration Examples The following example configures the maximum number of multicast groups to 100 on the megabit interface 0/1:

```
Hostname(config)# interface Ethernet 0/1
Hostname(config-if)# ip igmp snooping max-group 100
```

Platform Description N/A

2.14 ip igmp snooping mrouter learn pim-dvmrp

Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface

Use the **no** form of this command to disable the dynamic learning.

Use the **default** form of this command to restore the default setting.

ip igmp snooping mrouter learn pim-dvmrp

no ip igmp snooping mrouter learn pim-dvmrp

default ip igmp snooping [**vlan** *vid*] **mrouter learn pim-dvmrp**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled).
By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

Configuration Examples The following example enables the dynamic routing interface learning function on VLAN 1.

```
Hostname(config)# no ip igmp snooping mrouter learn pim-dvmrp
Hostname(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Platform Description N/A

2.15 ip igmp snooping preview

Use this command to allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.
Use **no** or **default** form of this command to disable multicast preview.
ip igmp snooping preview *profile-number*
no ip igmp snooping preview
default ip igmp snooping preview

Parameter Description

Parameter	Description
profile-number	Profile number (1-1024)

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.

Configuration Examples The following example associates the profile 2 to the Ethernet 0/1 and associates multicast preview with profile 1.

```
Hostname(config)# ip igmp snooping preview 1
Hostname(config-if)# int Ethernet 0/1
Hostname(config-if)# ip igmp snooping filter 2
```

Platform Description N/A

2.16 ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.
Use **no** or **default** form of this command to restore the default setting.
ip igmp snooping preview interval *seconds*
no ip igmp snooping preview interval
defaut ip igmp snooping preview interval

Parameter Description

Parameter	Description
seconds	Preview interval from 1 to 300 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:

```
Hostname(config)# ip igmp snooping preview 1
Hostname(config)# ip igmp snooping preview interval 100
```

Platform Description N/A

2.17 ip igmp snooping querier

Use this command to enable the IGMP querier.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping querier

no ip igmp snooping querier

default ip igmp snooping [**vlan** *vid*] **querier**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.

If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

Configuration Examples The following example enables the IGMP querier function in VLAN 2.

```
Hostname(config)# ip igmp snooping querier
Hostname(config)# ip igmp snooping vlan 2 querier
```

Platform Description N/A

2.18 ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.

Use **no** or **default** form of this command to remove the source IP address configured.

ip igmp snooping [**vlan** *vid*] **querier address** *a.b.c.d*

no ip igmp snooping [**vlan** *vid*] **querier address**

default ip igmp snooping [**vlan** *vid*] **querier address**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.
a.b.c.d	Source IP address of the IGMP querier

Defaults N/A

Command Mode Global configuration mode

Usage Guide After enabling IGMP querier, you msut configure a source IP address for the IGMP querier to activate this function..
If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

Configuration Examples The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device.

```
Hostname(config)# ip igmp snooping querier address 1.1.1.1
```

The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3.

```
Hostname(config)# ip igmp snooping vlan 3 querier address 1.1.1.1
```

Platform Description

2.19 ip igmp snooping querier max-response-time

Use this command to configure the maximum response time of the IGMP querier.
Use **no** or **default** form of this command to restore to the default setting.
ip igmp snooping [**vlan** *vid*] **querier max-response-time** *seconds*
no ip igmp snooping [vlan *vid* **] querier max-response-time**
default ip igmp snooping [**vlan** *vid*] **querier max-response-time**

Parameter Description

Parameter	Description
num	Maximum response time from 1 to 25 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples The following example specifies the maximum response time of the IGMP querier on the device.

```
Hostname(config)# ip igmp snooping querier max-response-time 15
```

The following example specifies the maximum response time of the IGMP querier in VLAN 3.

```
Hostname(config)# ip igmp snooping vlan 3 querier max-response-time 15
```

Platform N/A

Description

2.20 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping querier query-interval *seconds*

no ip igmp snooping querier query-interval

default ip igmp snooping [**vlan** *vid*] **querier query-interval**

Parameter Description

Parameter	Description
seconds	Query interval from 1 to 18,000 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples The following example configures the query interval on the device.

```
Hostname(config)# ip igmp snooping querier query-interval 100
```

The following example configures the query interval in VLAN 3.

```
Hostname(config)# ip igmp snooping vlan 3 querier query-interval 100
```

Platform Description N/A

2.21 ip igmp snooping querier timer expiry

Use this command to specify the expiration timer for non-querier.

Use **no** form of this command to restore the default setting.

ip igmp snooping [**vlan** *vid*] **querier timer expiry** *seconds*

ip igmp snooping [**vlan** *vid*] **querier timer expiry** *seconds*

default ip igmp snooping [**vlan** *vid*] **querier timer expiry**

Parameter Description

Parameter	Description
seconds	Theexpiration timer from 60 to 300 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default is 125 seconds.

Command Mode Global configuration mode

Usage Guide After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.
If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples The following example configures the non-querier expiration timer on the device.

```
Hostname(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
Hostname(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

Platform Description N/A

2.22 ip igmp snooping querier version

Use the following commands to specify IGMP Snooping querier version.
ip igmp snooping [**vlan** *vid*] **querier version 1**
ip igmp snooping [**vlan** *vid*] **querier version 2**
Use **no** or **default** form of this command to restore to the default setting.
no ip igmp snooping [**vlan** *vid*] **querier version**
default ip igmp snooping [**vlan** *vid*] **querier version**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default version is IGMPv2.

Command Mode Global configuration mode

Usage Guide If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.
IGMPv1 and IGMPv2 are supported.

Configuration Examples The following example configures IGMP querier version on the device.

```
Hostname(config)# ip igmp snooping querier version 1
```

The following example configures IGMP querier version on VLAN3.

```
Hostname(config)# ip igmp snooping vlan 3 querier version 1
```

Platform Description N/A

2.23 ip igmp snooping query-max-response-time

Use this command to specify the time for the switch to wait for the member join message after receiving the **query** message.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-resposne-time

default ip igmp snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	The aging time of the routing inerface that the switch learns dynamically, in the range from 1 to 65.535

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member.

This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.

Configuration Examples The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Hostname(config)# ip igmp snooping query-max-response-time 100
```

Platform Description N/A

2.24 ip igmp snooping suppression enable

Use this command to enable IGMP snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping suppression enable
no ip igmp snooping suppression enable
default ip igmp snooping suppression enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks.
This function is only supported on IGMPv1 and IGMPv2 reports.

Configuration Examples The following example enables IGMP snooping suppression on the device.

```
Hostname(config)# ip igmp snooping suppression enable
```

Platform Description N/A

2.25 ip igmp snooping svgl profile

Use this command to specify the multicast group address range applied in the SVGL/IVGL-SVGL mode.
Use the **no** or **default** form of this command to restore the default setting.
ip igmp snooping svgl profile *profile-number*
no ip igmp snooping svgl profile
default ip igmp snooping svgl profile

Parameter Description

Parameter	Description
profile-number	Profile number, in the range of 1-1,024

Defaults No profile is associated.

Command Mode Global configuration mode

Usage Guide When the IGMP Snooping works in the SVGL and IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode.

Configuration Examples The following example specifies the profile 2 applied in SVGL mode.

```
Hostname(config)# ip igmp snooping svgl profile 2
```

Platform Description N/A

2.26 ip igmp snooping svgl subvlan

Use this command to specify the subvlan of multicast VLAN.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping svgl subvlan [*vid-range*]

no ip igmp snooping svgl subvlan [*vid-range*]

default ip igmp snooping svgl subvlan [*vid-range*]

Parameter Description

Parameter	Description
vid-range	VLAN ID or range of VLAN ID

Defaults By default, all VLANs except shared VLANs serve as its sub VLANs.

Command Mode Global configuration mode

Usage Guide This command only takes effect in SVGL and IVGL-SVGL mode.

Configuration Examples The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.

```
Hostname(config)# ip igmp snooping svgl vlan 3
Hostname(config)# ip igmp snooping svgl subvlan 2,5-7
```

Platform Description N/A

2.27 ip igmp snooping svgl vlan

Use this command to specify the shared VLAN in SVGL mode.

Use the **no** form of this command to restore the default setting.

ip igmp snooping svgl vlan *vid*

no ip igmp snooping svgl vlan

default ip igmp snooping svgl vlan

Parameter Description

Parameter	Description

vid	VLAN ID

Defaults By default , the shared VLAN is VLAN 1.

Command Mode Global configuration mode

Usage Guide This command only works in the SVGL and IVGL-SVGL mode.

Configuration Examples The following example specifies the vlan2 as the shared vlan
The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.

```
Hostname(config)# ip igmp snooping svgl vlan 3
Hostname(config)# ip igmp snooping svgl subvlan 2,5-7
```

Platform Description N/A

2.28 ip igmp snooping tunnel

Use this command to enable 802.1Q tunneling (QinQ) support for IGMP Snooping.
Use the **no** or **default** form of this command to restore the default setting.
ip igmp snooping tunnel
no ip igmp snooping tunnel
default ip igmp snooping tunnel

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled.

Command Mode Global configuration mode

Usage Guide After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways:

- First: QinQ transmits IGMP packets transparently. Create multicast entries in the VLAN to which the IGMP packets belong, and forward IGMP packets in the VLAN.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of Port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed by Port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN

10.

- Second: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed Port A. When multicast requests of VLAN 10 are sent to Port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.
  By default, the second way is used.

Configuration Examples The following example enables QinQ support for IGMP Snooping.

```
Hostname(config)# ip igmp snooping tunnel
```

Platform Description N/A

2.29 ip igmp snooping vlan

Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode.
Use the **no** form of this command is used to disable the IGMP Snooping.
Use the **default** form of this command to restore the default setting.
ip igmp snooping vlan *vid*
no ip igmp snooping vlan *vid*
default ip igmp snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094

Defaults If IGMP Snooping (IVGL mode) is enabled globally, all VLANs are enabled with IGMP Snooping (IVGL mode).
If IGMP Snooping (IVGL mode) is not enabled globally, all VLANs are not enabeld with IGMP Snooping (IVGL mode).

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable the IGMP snooping on the specified vlan.

> ⚠ The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.

Configuration Examples The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

```
Hostname(config)# ip igmp snooping ivgl
Hostname(config)# no ip igmp snooping vlan 2
```

Platform Description N/A

2.30 ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.
Use the **no** form of this command to delete a static routing interface.
Use the **default** form of this command to restore the default setting.
ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*
no ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*
default ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094
interface-type interface-number	Interface ID

Defaults No static routing interface is configured by default.

Command Mode Global configuration mode

Usage Guide A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.
When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded.
When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

Configuration Examples The following example configures a static routing interface.

```
Hostname(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet 0/1
```

Platform Description N/A

2.31 ip igmp snooping vlan static interface

Use this command to configure a static member interface of a multicast group.

Use the **no** form of this command to delete a static member interface from a multicast group.
Use the **default** form of this command to restore the default setting.
ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*
no ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*
default ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094
ip-addr	Multicast IP address
interface-id	Interface ID

Defaults No static member interface of any multicast group is configured by default.

Command Mode Global configuration mode

Usage Guide The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

Configuration Examples The following example configures a static member interface for the multicast group 224.1.1.1.

```
Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
GigabitEthernet 0/1
```

Platform Description N/A

2.32 permit

Use this command to permit the multicast forwarding for specified ranges of a specified profile.
permit

Parameter Description

Parameter	Description
N/A	N/A

Defaults The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode Profile configuration mode

Usage Guide A profile is used to filter a group of multicast packets, so as to assist other features.

Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.
3. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1.

```
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244
Hostname(config-profile)# permit
```

Platform Description N/A

2.33 range

Use this command to define a range for a specific profile.

Use the **no** form of the command to remove the range from the profile.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter Description

Parameter	Description
low-ip-address	Start address of a range
high-ip-address	End address of a range

Defaults No range is defined for a profile by default.

Command Mode Profile configuration mode

Usage Guide A profile is used to filter a group of multicast packets, so as to assist other features.

Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.
3. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples The following is an example of allowingpermits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244: of profile 1.

```
Hostname(config)# ip igmp profile 1
Hostname(config-profile)# range 224.2.2.2 224.2.2.244224.2.2.2
Hostname(config-profile)# permit
```

Platform Description N/A

2.34 show ip igmp profile

Use this command to display the profile information.

show ip igmp profile

show ip igmp profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Displays configuration information of the designated profile.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the profile information.

Configuration Examples The following example displays the profile information.

```
Hostname(config-if)# show ip igmp profile
Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

2.35 show ip igmp snooping

Use this command to display related information of IGMP Snooping.

show ip igmp snooping [**gda-table** | **interfaces** *interface-type interface-number* | **mrouter**| **statistics** [**vlan** *vlan-id*] | **querier** [**detail | vlan** *vid*] | **user-info**]

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By defualt, IGMP Snooping information of all VLANs are displayed.
interface-type interface-number	Interface type and number

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples The following example displays global IGMP Snooping information.

```
Hostname#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

The following example displays VLAN1 IGMP Snooping information.

```
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 Response 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
```

Platform Description N/A

Security Configuration Commands

1 AAA Commands

2 RADIUS Commands

3 TACACS+ Commands

4 802.1X Commands

5 Web Authenticatoin Commands

6 SCC Commands

7 Global IP-MAC Binding Commands

8 Password-Policy Commands

9 Storm Control Commands

10 SSH Commands

11 CPU Protection Commands

12 DHCP Snooping Commands

13 DAI Commands

14 IP Source Guard Commands

15 NFPP Commands

1 AAA Commands

1.1 aaa accounting commands

Use this command to configure NAS command accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting commands *level* **{ default |** *list-name* **} start-stop** *method1* [*method2*…]

no aaa accounting commands *level* { **default |** *list-name* }

Parameter Description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
default	When this parameter is used, the following defined method list is used as the default method for command accounting.
list-name	Name of the command accounting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.
The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples The following example enables NAS command accounting.

```
Hostname(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.
accounting commands	Applies the accounting commands to the terminal line.

Platform Description N/A

1.2 aaa accounting exec

Use this command to enable NAS access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting exec { **default |** *list-name* } **start-stop** *method1* [*method2...*]

no aaa accounting exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
list-name	Name of the Exec accounting method list, which could be any character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system enables the exec accounting function after enabling the login authentication.

After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples The following example enables NAS access accounting.

```
Hostname(config)# aaa accounting network start-stop group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.
accounting commands	Applies the Exec accounting to the terminal line.

Platform Description N/A

1.3 aaa accounting network

Use this command to enable network access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting network { default | *list-name* **} start-stop** *method1* [*method2*..]

no aaa accounting network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
list-name	Name of the accounting method list
method	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system performs accounting of user activities by sending record attributes to the security server.

Use the **start-stop** keyword to set the user accounting option.

Configuration Examples The following example enables network access accounting.

```
Hostname(config)# aaa accounting network start-stop group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization network	Defines a network authorization method list.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

Platform Description N/A

1.4 aaa accounting update

Use this command to enable the accounting update function.

Use the **no** form of this command to restore the default setting.

aaa accounting update

no aaa accounting update

Parameter Description N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples The following example enables the accounting update function.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description N/A

1.5 aaa accounting update periodic

Use this command to set the interval of sending the accounting update message.

Use the **no** form of this command to restore the default setting.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter Description

Parameter	Description
interval	Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute.

Defaults The default is 5 minutes.

Command Global configuration mode

Mode

Usage Guide If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples The following example sets the interval of accounting update to 1 minute.

```
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update
Hostname(config)# aaa accounting update periodic 1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description N/A

1.6 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list.

Use the **no** form of this command to delete the 802.1x user authentication method list.

aaa authentication dot1x { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication dot1x { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
list-name	Name of the 802.1x user authentication method list, which could be any character string
method	It must be one of the keywords: **local**, **none** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the **aaa authentication dot1x** command to configure a default or optional method list for 802.1x user authentication.
The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication dot1x rds_d1x group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
dot1x authentication	Associates a specific method list with the 802.1x user.
username	Defines a local user database.

Platform Description N/A

1.7 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.
Use the **no** form of this command to delete the user authentication method list.
aaa authentication enable default *method1* [*method2*...]
no aaa authentication enable default

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
method	It must be one of the keywords: **local, none** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
enable	Enables AAA Enable authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable

authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.
The next method can be used for authentication only when the current method does not work.
The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Configuration Examples The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication enable default group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
enable	Switchover the user level.
username	Defines a local user database.

Platform Description N/A

1.8 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.
Use the **no** form of this command to delete the authentication method list.
aaa authentication login { **default** | *list-name* } *method1* [*method2*..]
no aaa authentication login { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **group** and **subs**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
subs	Uses the subs database for authentication.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.
The next method can be used for authentication only when the current method does not work.
You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Configuration Examples The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication login list-1 group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

Platform Description N/A

1.9 aaa authentication web-auth

Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.
Use the **no** form of this command to delete the authentication method list.
aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]
no aaa authentication web-auth { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication.
list-name	Name of second-generation Web authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the **aaa authentication web-auth** command to configure a default or optional method list for user authentication.
The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named **rds_web**. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication web-auth rds_web group radius none
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI.
Use the **no** form of this command to restore the default setting.
aaa authorization commands *level* { **default** | *list-name* } *method1* [*method2*...]
no aaa authorization commands *level* { **default** | *list-name* }

Parameter Description

Parameter	Description
level	Command level to be authorized in the range from 0 to 15
default	When this parameter is used, the following defined method list is used as the default method for command authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Do not perform authorization.
group	Uses the server group for authorization. At present, the TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.
It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.
The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

Configuration Examples The following example uses the TACACS+ server to authorize the level 15 command.

```
Hostname(config)# aaa authorization commands 15 default group tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization commands	Applies the command authorization for the terminal line.

Platform Description N/A

1.11 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).
Use the **no** form of this command to restore the default setting.
aaa authorization config-commands
no aaa authorization config-commands

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

Configuration Examples The following example enables the configuration command authorization function.

```
Hostname(config)# aaa authorization config-commands
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.

Platform Description N/A

1.12 aaa authorization console

Use this command to authorize the commands of the users who have logged in the console.

Use the **no** form of this command to restore the default setting.

aaa authorization console

no aaa authorization console

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

Configuration Examples The following example enables the aaa authorization console function.

```
Hostname(config)# aaa authorization console
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.
	authorization commands	Applies the command authorization to the terminal line.

Platform Description N/A

1.13 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level.

Use the **no** form of this command to restore the default setting.

aaa authorization exec { **default** | *list-name* } *method1* [*method2*...]
no aaa authorization exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
local	Uses the local user name database for authorization.
none	Does not perform authorization.
group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Configuration Examples The following example uses the RADIUS server to authorize Exec.

```
Hostname(config)# aaa authorization exec default group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization exec	Applies the command authorization to the terminal line.
username	Defines a local user database.

Platform Description N/A

1.14 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.
Use the **no** form of this command to restore the default setting.
aaa authorization network { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
method	It must be one of the keywords: none and group. One method list can contain up to four methods.
none	Does not perform authorization.
group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The system supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.
Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.
The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Configuration Examples The following example uses the RADIUS server to authorize network services.

```
Hostname(config)# aaa authorization network default group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting	Defines AAA accounting.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

Platform Description N/A

1.15 aaa domain

Use this command to configure the domain attributes.
Use the **no** form of this command to restore the default setting.
aaa domain { **default** | *domain-name* }

no aaa domain { **default |** *domain-name* }

Parameter Description

Parameter	Description
default	Uses this parameter to configure the default domain.
domain-name	The name of the specified domain

Defaults No domain is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Configuration Examples The following example configures the domain name.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)#
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

1.16 aaa domain enable

Use this command to enable domain-name-based AAA service.
Use the **no** form of this command to restore the default setting.
aaa domain enable
no aaa domain enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide To perform the domain-name-based AAA service configuration, enable this service.

Configuration Examples The following example enables the domain-name-based AAA service.

```
Hostname(config)# aaa domain enable
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
show aaa doamain	Displays the domain configuration.

Platform Description N/A

1.17 aaa local authentication attempts

Use this command to set login attempt times.

aaa local authentication attempts *max-attempts*

Parameter Description

Parameter	Description
max-attempts	In the range from 1 to 2,147,483,647

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use this command to configure login attempt times.

Configuration Examples The following example sets login attempt times to 6.

```
Hostname #configure terminal
Hostname(config)#aaa local authentication attempts 6
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description N/A

1.18 aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.

aaa local authentication lockout-time *lockout-time*

Parameter Description	Parameter	Description
	lockout-time	In the range from 1 to 2,147,483,647 in the unit of minutes

Defaults The default is 15 minutes.

Command Mode Global configuration mode

Usage Guide Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

Configuration Examples The following example sets the lockout-time period to 5 minutes.

```
Hostname#configure terminal
Hostname(config)#aaa local authentication lockout-time 5
```

Related Commands	Command	Description
	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description N/A

1.19 aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success.
Use the **no** form of this command to restore the default setting.
aaa log enable
no aaa log enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the system to print the syslog informing aaa authentication success.

Configuration Examples The following example disables the system to print the syslog informing aaa authentication success.

```
Hostname(config)# no aaa log enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.20 aaa log rate-limit

Use this command to set the rate of printing the syslog informing AAA authentication success.

Use the **no** form of this command to restore the default printing rate.

aaa log rate-limit *num*

no aaa log rate-limit

Parameter Description	Parameter	Description
	num	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.

Defaults The default is 5.

Command Mode Global configuration mode

Usage Guide

Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

Configuration Examples The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
Hostname(config)# aaa log rate-limit 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.21 aaa new-model

Use this command to enable the AAA security service.

Use the **no** form of this command to restore the default setting.

aaa new-model

no aaa new-model

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

Configuration Examples The following example enables the AAA security service.

```
Hostname(config)# aaa new-model
```

Related Commands	Command	Description
	aaa authentication	Defines a user authentication method list.
	aaa authorization	Defines a user authorization method list.
	aaa accounting	Defines a user accounting method list.

Platform Description N/A

1.22 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users.

Use the **no** form of this command to restore the default setting.

access-limit *num*

no access-limit

Parameter Description	Parameter	Description
	num	The number used for the user limitation is only valid for the IEEE802.1 users.

Defaults By default, no number of users is limited.

Command Mode Domain configuration mode

Usage Guide This command limits the number of users for the domain.

Configuration Examples The following example sets the number of users to 20 for the domain named test.com.

```
Hostname(config)# aaa domain test.com
```

```
Hostname(config-aaa-domain)# access-limit 2
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Switchover the user level.
	show aaa domain	Defines a local user database.

Platform Description N/A

1.23 accounting network

Use this command to configure the Network accounting list.

Use the **no** form of this command to restore the default setting.

accounting network { **default** | *list-name* }

no accounting network

Parameter Description	Parameter	Description
	default	Uses this parameter to specify the default method list.
	list-name	The name of the network accounting list

Defaults With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

Command Mode Domain configuration mode

Usage Guide Use this command to configure the Network accounting method list for the specified domain.

Configuration Examples The following example sets the Network accounting method list for the specified domain.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)# accounting network default
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform Description N/A

1.24 authentication dot1x

Use this command to configure the IEEE802.1x authentication list.

Use the **no** form of this command to restore the default setting.

authentication dot1x { **default** | *list-name* }

no authentication dot1x

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list
list-name	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Mode Domain configuration mode

Usage Guide Specify an IEEE802.1x authentication method list for the domain.

Configuration Examples The following example sets an IEEE802.1x authentication method list for the specified domain.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)# authentication dot1x default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

1.25 authorization network

Use this command to configure the Network authorization list.

Use the **no** form of this command to restore the default setting.

authorization network { **default** | *list-name* }

no authorization network

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list.
list-name	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default

method list for users.

Command Mode Domain configuration mode

Usage Guide Specify an authorization method list for the domain.

Configuration Examples The following example sets an authorization method list for the specified domain.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)# authorization network default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

1.26 clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout { **all | user-name** *word* }

Parameter Description

Parameter	Description
all	Indicates all locked users.
user-name *word*	Indicates the ID of the locked User.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all the user lists or a specified user list.

Configuration Examples The following example clears the lockout user list.

```
Hostname(config)# clear aaa local user lockout all
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform N/A

Description

1.27 show aaa accounting update

Use this command to display the accounting update information.

show aaa accounting update

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the accounting update interval and whether the accounting update is enabled.

Configuration Examples The following example displays the accounting update information.

```
Hostname# show aaa accounting update
```

Related Commands	**Command**	**Description**
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.

Platform Description N/A

1.28 show aaa domain

Use this command to display all current domain information.

show aaa domain [**default** | *domain-name*]

Parameter Description	**Parameter**	**Description**
	default	Displays the default domain.
	domain-name	Displays the specified domain.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide If no domain-name is specified, all domain information will be displayed.

Configuration Examples The following example displays the domain named domain.com.

```
Hostname(config)# 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
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.

Platform Description N/A

1.29 show aaa group

Use this command to display all the server groups configured for AAA.

show aaa group

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following command displays all the server groups.

```
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
```

Related Commands	Command	Description
	aaa group server	Configures the AAA server group.

Platform Description N/A

1.30 show aaa lockout

Use this command to display the lockout configuration.

show aaa lockout

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the lockout configuration.

Configuration Examples The following example displays the lockout configuration.

```
Hostname# show aaa lockout
Lock tries:   3
Lock timeout:  15 minutes
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.31 show aaa method-list

Use this command to display all AAA method lists.

show aaa method-list

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode/Global configuration mode/Interface configuration mode

Mode

Usage Guide Use this command to display all AAA method lists.

Configuration Examples The following example displays the AAA method list.

```
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 authorization network default group radius
```

Related Commands

Command	Description
aaa authentication	Defines a user authentication method list
aaa authorization	Defines a user authorization method list
aaa accounting	Defines a user accounting method list

Platform Description N/A

1.32 show aaa user

Use this command to display AAA user information.

show aaa user { all | lockout | by-id *session-id* **| by-name** *user-name* **}**

Parameter Description

Parameter	Description
all	Displays all AAA user information.
lockout	Displays the locked AAA user information.
by-id *session-id*	Displays the information of the AAA user that with a specified session ID.
by-name *user-name*	Displays the information of the AAA user with a specified user name.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display AAA user information.

Configuration Examples The following example displays AAA user information.

```
Hostname#show aaa user all

------------------------------

      Id ----- Name

 2345687901     wwxy

------------------------------

Hostname# show aaa user by-id 2345687901

------------------------------

      Id ----- Name

 2345687901     wwxy

Hostname# show aaa user by-name wwxy

------------------------------

      Id ----- Name

 2345687901     wwxy

------------------------------


Hostname# show aaa user lockout


Name                          Tries     Lock      Timeout(min)

------------------------------- ---------- ---------- ------------

Hostname#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.33 state

Use this command to set whether the configured domain is valid.

Use the **no** form of this command to restore the default setting.

state { **block | active** }

no state

Parameter Description	Parameter	Description
	block	The configured domain is invalid.

active	The configured domain is valid.

Defaults The default is active.

Command Mode Domain configuration mode

Usage Guide Use this command to set whether the specified configured domain is valid.

Configuration Examples The following example sets the configured domain to be invalid.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)# state block
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain enable	Displays the domain configuration.

Platform Description N/A

1.34 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Use the **no** form of this command to restore the default setting.

username-format { **without-domain** | **with-domain** }

no username-format

Parameter Description

Parameter	Description
without-domain	Sets the user name without the domain information.
with-domain	Sets the user name with the domain information.

Defaults The default is without-domain.

Command Mode Domain configuration mode

Usage Guide Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Configuration Examples The following example sets the user name without the domain information.

```
Hostname(config)# aaa domain test.com
Hostname(config-aaa-domain)# username-domain without-domain
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform Description N/A

2 RADIUS Commands

2.1 aaa group server radius

Use this command to enter AAA server group configuration mode.

Use the **no** form of this command to restore the default setting.

aaa group server radius *name*

no aaa group server radius *name*

Parameter Description

Parameter	Description
name	Server group name. Keywords “radius” and “tacacs +” are excluded as they are the default RADIUS and TACACS+ server group names.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure a RADIUS AAA server group.

Configuration Examples The following example configures a RADIUS AAA server group named ss.

```
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# end
Hostname# show aaa group
Type      Reference  Name
---------- ---------- ----------
radius    1         radius
tacacs+   1         tacacs+
radius    1         ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface-name*

no radius source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface that the source IP address of the RADIUS packet belongs to.

Defaults The source IP address of the RADIUS packet is set by the network layer.

Command mode Global configuration mode

Usage Guide In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Configuration Examples The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet.

```
Hostname(config)# ip radius source-interface fastEthernet 0/0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.
ip address	Configures the IP address of the interface.

Platform Description N/A

2.3 radius attribute

Use this command to set the private attribute type value.

Use the **no** form of this command to restore the default setting.

radius attribute { *id* **| down-rate-limit | dscp | mac-limit | up-rate-limit** } **vendor-type** *type*

no radius attribute { *id* | **down-rate-limit** | **dscp** | **mac-limit | up-rate-limit** } **vendor-type**

Parameter Description

Parameter	Description
id	Function ID, in the range from 1 to 255
type	Private attribute type, in the range from 1

	to 255.

Defaults Only the default configuration of private attributes is recognized.

id	Function	type
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
2	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	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Extended attributes:

id	Function	type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5

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	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command Mode Global configuration mode

Usage Guide This command is used to configure the private attribute type value.

Configuration Examples The following example sets the type of max up-rate to 211.

```
Hostname(config)# radius attribute 16 vendor-type 211
```

Related Commands

Command	Description
radius set qos cos	Sets the qos value sent by the RADIUS server as the cos value of the interface.

Platform Description N/A

2.4 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface.
Use the **no** form of this command to restore the default setting.
radius set qos cos
no radius set qos cos

Parameter Description

Parameter	Description
N/A	N/A

Defaults Set the QoS value sent by the RADIUS server as the DSCP value.

Command Mode Global configuration mode.

Usage Guide This command is used to set the QoS value sent by the RADIUS server as the CoS value, and the DSCP value by default.

Configuration Examples The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
Hostname(config)# radius set qos cos
```

Related Commands

Command	Description
radius vendor-specific extend	Extends RADIUS as not to differentiate the IDs of private vendors.

Platform Description N/A

2.5 radius support cui

Use this command to enable RADIUS to support the cui function.
Use the **no** form of this command to restore the default setting.
radius support cui
no radius support cui

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable RADIUS to support the cui function.

Configuration Examples The following example enables RADIUS to support the cui function.

```
Hostname(config)# radius support cui
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.6 radius user-name compatible

Use this command to configure the encapsulation format of a compatible user name.
Use the **no** form of this command to restore the default setting.
radius user-name compatible
no radius user-name compatible

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function to configure the encapsulation format of a user name is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After the function is enabled, the user name in a RADIUS packet is encapsulated using the format sent by the client, instead of UTF-8.

Configuration Examples The following example enables the function to configure the encapsulation format of a user name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius user-name compatible
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

2.7 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

Use the **no** form of this command to restore the default setting.

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description

Parameter	Description
N/A	N/A

Defaults Only the private vendor IDs are recognized.

Command Mode Global configuration mode

Usage Guide This command is used to identify the attributes of all vendor IDs by type.

Configuration Examples The following example extends RADIUS so as not to differentiate the IDs of private vendors:

```
Hostname(config)# radius vendor-specific extend
```

Related Commands

Command	Description
radius attribute	Configures vendor type.
radius set qos cos	Sets the QoS value sent by the RADIUS server as the cos value of the interface.

Platform Description N/A

2.8 radius-server account attribute

Use this command to enable account-request packets to contain a specified RADIUS attribute.

Use the **no** or **default** form of this command to restore the default setting.
radius-server account attribute *type* **package**
no radius-server account attribute *type* **package**
default radius-server account attribute *type* **package**

Use this command to disable account-request packets to contain a specified RADIUS attribute.
Use the **no** or **default** form of this command to restore the default setting.
radius-server account attribute *type* **unpackage**
no radius-server account attribute *type* **unpackage**
default radius-server account attribute *type* **unpackage**

Parameter Description

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults RFC-compliant

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable account-request packets to contain a specified RADIUS attribute.

Configuration Examples The following example disables account-request packets to contain attribute NAS-PORT-ID.

```
Hostname(config)# radius-server account attribute 87 unpackage
```

Platform Description N/A

2.9 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the second generation Web authentication user.
Use the **no** form of this command to disable this function.
radius-server account update retransmit
no radius-server account update retransmit

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.

Configuration Examples The following example configures accounting update packet retransmission for the second generation Web authentication user.

```
Hostname(config)#radius-server account update retransmit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 radius-server account vendor

Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.

Use the **no** or **default** form of this command to restore the default setting.

radius-server account vendor *vendor_name* **package**

no radius-server account vendor *vendor_name* **package**

default radius-server account vendor *vendor_name* **package**

Parameter Description

Parameter	Description
vendor_name	**cmcc/ microsoft/cisco**

Defaults Account-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.

Configuration Examples The following example enables account-request packets to contain “cmcc”.

```
Hostname(config)# radius-server account vendor cmcc package
```

Platform Description N/A

2.11 radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes.

Use the **no** form of this command to restore the default setting.

radius-server attribute class

no radius-server attribute class

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is required if the server pushes the flow control through the CLASS attribute.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.12 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.

Use the **no** form of this command to restore the default setting.

radius-server attribute 31 mac format { **ietf** | **normal** | **unformatted** }

no radius-server attribute 31 mac format

Parameter Description

Parameter	Description
ietf	The standard format specified by the IETF RFC3580. '-'is used as the separator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. ;.'is used as the separator. For example: 00d0.f833.22ac.
unformatted	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

Defaults The default format is unformatted.

Command Mode Global configuration mode

Usage Guide Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Configuration Examples The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

```
Hostname(config)# radius-server attribute 31 mac format ietf
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.

Platform Description N/A

2.13 radius-server authentication attribute

Use this command to enable access-request packets to contain a specified RADIUS attribute.
Use the **no** or **default** form of this command to restore the default setting.
radius-server authentication attribute *type* **package**
no radius-server authentication attribute *type* **package**
default radius-server authentication attribute *type* **package**

Use this command to disable access-request packets to contain a specified RADIUS attribute.
Use the **no** or **default** form of this command to restore the default setting.
radius-server authentication attribute *type* **unpackage**
no radius-server authentication attribute *type* **unpackage**
default radius-server authentication attribute *type* **unpackage**

Parameter Description

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults RFC-compliant

Command Mode Global configuration mode

Usage Guide Use this command to enable access-request packets to contain a specified RADIUS attribute.

Configuration Examples The following example disables access-request packets to contain attribute NAS-PORT-ID.

```
Hostname(config)# radius-server authentication attribute 87 unpackage
```

Platform Description N/A

2.14 radius-server authentication vendor

Use this command to enable access-request packets to contain vendor-specific RADIUS attributes.
Use the **no** or **default** form of this command to restore the default setting.
radius-server authentication vendor *vendor_name* **package**
no radius-server authentication vendor *vendor_name* **package**

default radius-server authentication vendor *vendor_name* **package**

Parameter Description

Parameter	Description
vendor_name	**cmcc/ microsoft/cisco**

Defaults Access-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.

Configuration Examples The following example enables access-request packets to contain “cmcc”.

```
Hostname(config)# radius-server authentication vendor cmcc package
```

Platform Description N/A

2.15 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the Radius server is unreachable.
Use the **no** form of this command to restore the default setting.
radius-server dead-criteria { **time** *seconds* [**tries** *number*] **| tries** *number* }
no radius-server dead-criteria { **time** [**tries**] **| tries** }

Parameter Description

Parameter	Description
time *seconds*	Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
tries *number*	Configures the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.

Defaults The default **time** *seconds* is 60 and **tries** *number* is 10.

Command Mode Global configuration mode

Usage Guide If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Configuration Examples The following example sets the timeout to 120 seconds and timeout times to 20.

```
Hostname(config)# radius-server dead-criteria time 120 tries 20
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable Radius server.
radius-server timeout	Defines the timeout for the packet re-transmission.

Platform Description N/A

2.16 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server.
Use the **no** form of this command to restore the default setting.
radius-server deadtime *minutes*
no radius-server deadtime

Parameter Description

Parameter	Description
minutes	Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes.

Defaults The default value of minutes is 0, that is, the device keeps sending requests to the unreachable Radius server.

Command Mode Global configuration mode

Usage Guide If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.

Configuration Examples The following example sets the duration when the device stops sending requests to 1 minute.

```
Hostname(config)# radius-server deadtime 1
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server dead-criteria	Defines the criteria to determine that a Radius server is unreachable.

Platform Description N/A

2.17 radius-server host

Use this command to specify a RADIUS security server host.
Use the **no** form of this command to restore the default setting.
radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
no radius-server host { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv6 address of the RADIUS security server host.
ipv6-address	IPv4 address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
port-number	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.
port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username *name*	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
idle-time *time*	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disables the detection to the authentication port on the

	RADIUS security server. It is enabled by default.
key [**0** | **7**] *text-string*	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

Defaults No RADIUS host is specified by default.

Command Mode Global configuration mode

Usage Guide In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Configuration Examples The following example defines a RADIUS security server host:

```
Hostname(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Hostname(config)# radius-server host 192.168.100.1 test username viven
idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Hostname(config)# radius-server host 3000::100
```

Related Commands

Command	Description
aaa authentication	Defines the AAA authentication method list
radius-server key	Defines a shared password for the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.

Platform Description N/A

2.18 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

Use the **no** form of this command to restore the default setting.

radius-server key [**0 | 7**] *text-string*

no radius-server key

Parameter Description

Parameter	Description
text-string	Text of the shared password
0 | 7	Password encryption type. 0: no encryption; 7: Simply-encrypted.

Defaults No shared password is specified by default.

Command Mode Global configuration mode.

Usage Guide A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Configuration Examples The following example defines the shared password **aaa** for the RADIUS security server:

```
Hostname(config)# radius-server key aaa
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server timeout	Defines the timeout for the RADIUS packet.

Platform Description N/A

2.19 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.
Use the **no** form of this command to restore the default setting.
radius-server retransmit *retries*
no radius-server retransmit

Parameter Description

Parameter	Description
retries	Number of retransmissions in the range from 0 to 100. The value of 0 indiecates no retransmission.

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Configuration Examples The following example sets the number of retransmissions to 4.

```
Hostname(config)# radius-server retransmit 4
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout for the RADIUS packet.

Platform Description N/A

2.20 radius-server source-port

Use this command to configure the source port to send RADIUS packets.
Use the **no** form of this command to restore the default setting.
radius-server source-port *port*
no radius-server source-port

Parameter Description

Parameter	Description
port	The port ID, in the range from 0 to 65535.

Defaults The default is a random number.

Command Mode Global configuration mode

Usage Guide The source port is random by default. This command is used to specify a source port.

Configuration Examples The following example configures source port 10000 to send RADIUS packets.

```
Hostname(config)# radius-server source-port 10000
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

2.21 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.
Use the **no** form of this command to restore the default setting.
radius-server timeout *seconds*
no radius-server timeout

Parameter Description	Parameter	Description
	seconds	Timeout in the range from 1 to 1,000 in the unit of seconds.

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to change the timeout of packet retransmission.

Configuration Examples The following example sets the timeout to 10 seconds.

```
Hostname(config)# radius-server timeout  10
```

Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server retransmit	Defines the number of the RADIUS packet retransmissions.
	radius-server key	Defines a shared password for the RADIUS server.

Platform Description N/A

2.22 server auth-port acct-port

Use this command to add the server of the AAA server group.
Use the **no** form of this command to restore the default setting.

server { *ipv4-addr* | *ipv6-addr*} [**auth-port** *port1*] [**acct-port** *port2*]
no server { *ipv4-addr* | *ipv6-addr*} [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description

Parameter	Description
ip-addr	Server IP address
Ipv6-addr	Server IPv6 address
port1	Server authentication port
port2	Server accounting port

Defaults No server is configured by default.

Command Mode Server group configuration mode

Usage Guide N/A

Configuration Examples The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Hostname(config-gs-radius)# end
Hostname# show aaa group
Type      Reference  Name
---------- ---------- ----------
radius    1         radius
tacacs+   1         tacacs+
radius    1         ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.23 show radius acct statistics

Use this command to display RADIUS accounting statistics.

show radius acct statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays RADIUS accounting statistics.

```
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........
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.24 show radius attribute

Use this command to display standard Radius attributes.

show radius attribute

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays standard RADIUS attributes.

```
Hostname#sh 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
```

Platform Description N/A

2.25 show radius auth statistics

Use this command to display RADIUS authentication statistics.

show radius auth statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays RADIUS authentication statistics.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.26 show radius group

Use this command to display RADIUS server group configuration.

show radius group

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Global configuration mode/Privileged EXEC mode/Interface configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example displays RADIUS server group configuration.

```
Hostname#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
  Server key: test
  Authentication port:1812
  Accounting port:1813
  State:Active
```

Current products do not support the VRF parameter. The above example is for reference purpose. Please take the actual device as standard.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.27 show radius parameter

Use this command to display global RADIUS server parameters.

show radius parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays global RADIUS server parameters.

```
Hostname# show radius parameter
Server Timout:   5 Seconds
```

```
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:       10 Seconds
Tries:      10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 show radius server

Use this command to display the configuration of the RADIUS server.

show radius server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of the RADIUS server.

```
Hostname# show radius server
Server IP:   192.168.4.12
Accounting  Port:  23
Authen  Port:    77
Test Username:   viven
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
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform Description N/A

2.29 show radius vendor-specific

Use this command to display the configuration of the private vendors.

show radius vendor-specific

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the configuration of the private vendors.

Examples

```
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-version 17
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
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform Description

N/A

3 TACACS+ Commands

3.1 aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.
Use the **no** form of this command to remove a specified TACACS server group.
aaa group server tacacs+ *group_name*
no aaa group server tacacs+ *group_name*

Parameter Description

Parameter	Description
group_name	TACACS+ server group name, which cannot be **radius** or **tacacs+** The two names are the built-in group name.

Defaults No TACACS+ server group is configured.

Command Mode Global configuration mode

Usage Guide After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

Configuration Examples The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
Hostname(config)#aaa group server tacacs+ tac1
Hostname(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
server	Configures server list of TACACS+ server group.

Platform Description N/A

3.2 ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.
Use the **no** form of this command to disable use of the specified interface IP address.
ip tacacs source-interface *interface-name*
no ip tacacs source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface for the outgoing TACACS+ packets

Defaults The source IP address of TACACS+ packets is set on the network layer.

Command Mode Global configuration mode

Usage Guide To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.
This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices.

Configuration Examples The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets.

```
Hostname(config)# ip tacacs source-interface gigabitEthernet 0/0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ server.
ip address	Configures the IP address of an interface.

Platform Description N/A

3.3 server

Use this command to configure the IP address of the TACACS+ server for the group server.
Use the **no** form of this command to remove the TACACS+ server.
server { *ipv4-address* | *ipv6-address* }
no server { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the TACACS+ server
ipv6-address	IPv6 address of the TACACS+ server

Defaults No TACACS+ server is configured by default.

Command Mode TACACS+ server group configuration mode

Usage Guide You must configure the **aaa group server tacacs+** command before configuring this command.
To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode.
If there is no response from the first host entry, the next host entry is tried.

Configuration Examples The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group.

```
Hostname(config)#aaa group server tacacs+ tac1
Hostname(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures a TACACS+ server group.

Platform Description N/A

3.4 show tacacs

Use this command to display the TACACS+ server configuration.
show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the TACACS+ server configuration.

```
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
```

Related

Command	Description

Commands		
	tacacs-server host	Defines a TACACS+ secure server host.

Platform Description N/A

3.5 tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

tacacs-server host {*ipv4-address* | *ipv6-address*} [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]

no tacacs-server host { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the TACACS+ host
ipv6-address	IPv6 address of the TACACS+ host
port *integer*	Port number of the server. The range is from 1 to 65,535. The default is 49.
timeout *integer*	Timeout time of TACACS+ host. The range is from 1 to 1,000.
key *string*	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.

Defaults No TACACS+ host is specified by default.

Command Mode Global configuration mode

Usage Guide The TACACS+ host must be configured to implement AAA security service You can use this command to configure one or multiple TACACS+ hosts.

Configuration Examples The following example configures a TACACS+ host.

```
Hostname(config)# tacacs-server host 192.168.12.1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.6 tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server.
Use the **no** form of this command to remove the authentication encryption key.
tacacs-server key [**0** | **7**] *string*
no tacacs-server key

Parameter Description

Parameter	Description
string	Key string
0 | 7	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

Defaults No authentication encryption key is configured by default.

Command Mode Global configuration mode

Usage Guide Use command to configure a global authentication and encryption key for TACACS+ communication.
Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

Configuration Examples The following example defines the authentication encryption key of TACACS+ server as aaa:

```
Hostname(config)# tacacs-server key aaa
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ host.

Platform Description N/A

3.7 tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no** form of this command to restore the default timeout interval.
tacacs-server timeout *seconds*
no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout interval in the range from 1 to 1,000 in the unit of seconds

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

Configuration Examples The following example configures the timeout interval to 10 seconds.

```
Hostname(config)# tacacs-server timeout 10
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description N/A

4 802.1X Commands

4.1 aaa authorization ip-auth-mode

Use this command to set the IP authorization mode.

aaa authorization ip-auth-mode { disable | supplicant | radius-server | dhcp-server | mixed }

Parameter Description

Parameter	Description
disable	Disables IP authorization mode.
supplicant	Enables suppliant authorization mode.
radius-server	Enables Radius server authorization mode.
dhcp-server	Enables DHCP server authorization mode.
mixed	Enables mixed authorization mode.

Defaults IP authorization mode is disabled by default.

Command mode Global configuration mode

Usage Guide

Supplicant authorization mode supports only our company's supplicant.

Radius-server authorization mode requires the server to allocate IP addresses by framed-ip.

DHCP-server authorization mode requires the server to enable DHCP snooping or DHCP relay.

Mixed authorization mode supports multiple authorization methods.

Configuration Examples The following example enables suppliant authentication mode.

```
Hostname(config)# aaa authorization ip-auth-mode supplicant
```

Related Commands

Command	Description
show running-config	Displays the IP authentication mode.

Platform Description N/A

4.2 clear dot1x user all

Use this command to clear all the 802.1X authentication users.

clear dot1x user all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all the 802.1X authentication users.

Configuration Examples The following example clears all the 802.1X authentication users.

```
Hostname#clear dot1x user all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 clear dot1x user id

Use this command to clear 802.1X authentication users according to session IDs.

clear dot1x user id *session-id*

Parameter Description

Parameter	Description
session-id	Session ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear 802.1X authentication users according to session IDs.

Configuration Examples The following example clears an 802.1X authentication user whose session ID is 12345678.

```
Hostname#clear dot1x user id 12345678
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.4 clear dot1x user mac

Use this command to clear 802.1X authentication users according to MAC addresses.

clear dot1x user mac *mac-addr*

Parameter Description

Parameter	Description
mac-addr	MAC address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear 802.1X authentication users according to MAC addresses.

Configuration Examples The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A.

```
Hostname#clear dot1x user mac 0012.3456.789A
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.5 clear dot1x user name

Use this command to clear the 802.1 X authentication users according to the username.

clear dot1x user name *name-str*

Parameter Description

Parameter	Description
name-str	The username of the 802.1X authentication user

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the 802.1 X authentication users according to the username.

Configuration Examples The following example clears the 802.1X authentication user named 802.1X-user.

```
Hostname#clear dot1x user name dot1x-user
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 dot1x accounting

Use this command to configure the accounting list.

dot1x accounting *list-name*

Parameter Description

Parameter	Description
list-name	The name of the accounting list

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If AAA does not adopts 802.1X accounting as the default accounting method. Use this command to configure the 802.1X accounting method.

Configuration Examples The following example configures the accounting list.

```
Hostname(config)# dot1x accounting dot1x-acct
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 dot1x auth-address-table address

Use this command to configure the authentication address table.

dot1x auth-address-table address *mac-addr* **interface** *interface*

Parameter Description

Parameter	Description
mac-addr	The MAC address of the authentication host
interface	The interface of the authentication host

Defaults N/A

Command Mode Global configuration mode

Usage Guide Only the specified interface with the specified MAC address is able to pass the 802.1x authentication.

Configuration Examples The following example configures the authentication address table.

```
Hostname(config)# dot1x auth-address-table 00d0.f800.0cb2 interface
fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 dot1x authentication

Use this command to configure the authentication method list.

dot1x authentication *list-name*

Parameter Description

Parameter	Description
list-name	Authentication method list

Defaults N/A

Command Mode Global configuration mode

Usage Guide If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.

Configuration in WLAN security configuration mode is prior to that in global configuration mode.

Configuration Examples The following example configures the authentication method list

```
Hostname(config)# dot1x authentication dot1x-authen
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 dot1x auth-fail max-attempt

Use this command to set the maximum auth-attempts.

Use the **no** form of this command to restore the default setting.

dot1x auth-fail max-attempt *value*

no dot1x auth-fail max-attempt

Parameter Description	Parameter	Description
	value	The maximum auth-attempts. The value ranges from 1 to 3.

Defaults The default value is 3.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to adjust the maximum authentication attempts for those failed users.

Configuration Examples The following example sets the maximum auth-attempts to 2.

```
Hostname(config)# dot1x auth-fail max-attempt 2
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1x configuration.

Platform Description N/A

4.10 dot1x auth-fail vlan

Use this command to enable the auth-fail VLAN.

Use the **no** form of this command to restore the default setting.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

Parameter Description	Parameter	Description
	vlan-id	Auth-fail VLAN ID

Defaults No auth-fail VLAN is enabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to allow auth-fail users to access network by joining in a VLAN.

Configuration Examples The following example enables the auth-fail VLAN.

```
Hostname(config-if)# dot1x auth-fail vlan 30
```

Related Commands	Command	Description
	show dot1x interface	Displays the 802.1X configurations on the interface.

Platform Description N/A

4.11 dot1x auth-mode

Use this command to specify the 802.1X authentication mode.

dot1x auth-mode { **eap** | **chap** | **pap** }

Parameter Description	Parameter	Description
	eap	Enables EAP-MD5 authentication mode.
	chap	Enables CHAP authentication mode.
	pap	Enables PAP authentication mode.

Defaults The default is EAP-MD5 authentication mode.

Command Mode Global configuration mode

Usage Guide The selection of authentication mode depends on the suppliant and portal server.

Configuration Examples The following example enables CHAP authentication mode.

```
Hostname(config)# dot1x auth-mode chap
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.12 dot1x auth-with-order

Use this command to set the order and precedence for authentication.

dot1x auth-with-order

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Interface configuration mode

Mode

Usage Guide With this command executed, MAB authentication is initiated after 802.1X authentication fails. Meanwhile, MAB authentication takes precedence over 802.1X authentication.

Configuration Examples The following example sets the order and precedence for authentication.

```
Hostname(config-if)# dot1x auth-with-order
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.13 dot1x auto-req

Use this command to configure auto-request 802.1X authentication.

Use the **no** form of this command to restore the default setting.

dot1x auto-req

no dot1x auto-req

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Enable this function for MAB. If the authentication agent is already in the terminal system, enable it by clicking.

Configuration Examples The following example enables auto-request 802.1X authentication.

```
Hostname(config)# dot1x auto-req
```

Related Commands

Command	Description
show dot1x auto-req	Displays the automatic authentication request information.

Platform Description N/A

4.14 dot1x auto-req packet-num

Use this command to set the number of auto-request authentication packets.

dot1x auto-req packet-num *num*

Parameter Description

Parameter	Description
num	The number of auto-request authentication packets in the range from 0 to 1,000,000

Defaults The default is 0.

Command Mode N/A

Usage Guide N/A

Configuration Examples The following example sets the number of auto-request authentication packets to 100.

```
Hostname(config)# dot1x auto-req packet-num 100
```

Related Commands

Command	Description
show dot1x auto-req	Displays the authentication request information.

Platform Description N/A

4.15 dot1x auto-req req-interval

Use this command to set the auto-request authentication interval.

Use the **no** form of this command to restore the default setting.

dot1x auto-req req-interval *time*

no dot1x auto-req req-interval

Parameter Description

Parameter	Description
time	The auto-request authentication interval, in the range from 10 to 3,600 in the unit of seconds

Defaults The default is 30 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the auto-request authentication interval to 50 seconds.

Examples

```
Hostname(config)# dot1x auto-req req-interval 50
```

Related Commands

Command	Description
show dot1x auto-req	Displays the authentication request information.

Platform Description N/A

4.16 dot1x auto-req user-detect

Use this command to enable online user detection for auto-request authentication.

Use the **no** form of this command to disable online user detection for auto-request authentication.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables online user detection for auto-request authentication.

```
Hostname(config)# dot1x auto-req user-detect
```

Related Commands

Command	Description
show dot1x auto-req	Displays the authentication request information.

Platform Description N/A

4.17 dot1x client-probe enable

Use this command to enable online user probe function.

Use the **no** form of this command to restore the default setting.

dot1x client-probe enable

no do1x client-probe enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable online user probe function.

Configuration Examples The following example enables online user probe function.

```
Hostname(config)# dot1x client-probe enable
```

Related Commands	Command	Description
	show dot1x	Displays 802.1X configuration.

Platform Description N/A

4.18 dot1x critical

Use this command to enable the server IAB (Inaccessible Authentication Bypass) on the port.
Use the **no** form of this command to restore the default setting.
dot1x critical
no dot1x critical

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This functions is disabled by default.

Command Mode Interface configuration mode

Usage Guide With the IAB function enabled on the port, if there is only RADIUS authentication method in the 802.1X authentication method list and all RADIUS servers in this method list take no effect, the switch will set the network accessing authority for users by the IAB method, and send the EAPOL-SUCCESS packets to the users.

Configuration Examples The following example enables the server IAB (Inaccessible Authentication Bypass) function on the port.

```
Hostname(config-if-GigabitEthernet 0/5)#dot1x critical
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.19 dot1x critical recovery action reinitialize

Use this command to allow IAB users under the port to reinitialize authentication when the server has recovered.

Use the **no** form of this command to restore the default setting.

dot1x critical recovery action reinitialize

no dot1x critical recovery action reinitialize

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide After the port entering the inaccessible authentication bypass status, if the RADIUS server returns to normal, you need to reinitialize the authentication for all users that have accomplished the network access authorization through the inaccessible authentication bypass on ports in order to ensure the user legality.

Configuration Examples The following example allows IAB users under the port to reinitialize authentication when the server has recovered.

```
Hostname(config-if-GigabitEthernet 0/5)#dot1x critical recovery action
reinitialize
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.20 dot1x critical vlan

Use this command to configure the port in IAB status to jump to a specified auth-fail VLAN.

Use the **no** form of this command to disable this function.

dot1x critical vlan

no dot1x critical vlan

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide With this function enabled, if no user authentication is performed on the ports initially, after all RADIUS servers are invalidated, the user will initiate the authentication and the port will enter the IAB status and to be added to the VLAN configured. If this function is disabled, the VLAN of the port is not changed when the port is in the IAB status.

Configuration Examples
```
Hostname(config-if-GigabitEthernet 0/5)#dot1x critical vlan 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.21 dot1x dbg-filter

Use this command to enable debug information print for a user with a specified MAC address.
Use the **no** form of this command to clear the debug information.
dot1x dbg-filter *H.H.H*
no dot1x dbg-filter *H.H.H*

Parameter Description	Parameter	Description
	H.H.H	The MAC address of a user

Defaults Debug information of all authentication users is printed by default.

Command mode Global configuration mode

Usage Guide Use this command to print the debug information of a specific user If you want to locate the fault on the network where there are multiple users.

Configuration Examples The following example prints the debug information of the device with the specified MAC address.
```
Hostname(config)# dot1x dbg-filter 00d0.f800.0001
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.22 dot1x default

Use this command to restore 802.1X configuration to the default setting.

dot1x default

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to restore 802.1X configuration for quick re-configuration.

Configuration Examples The following example restores 802.1X configuration to the default setting.

```
Hostname(config)# dot1x default
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.23 dot1x default-user-limit

Use this command to set the maximum auth-user number on controlled interfaces.

Use the **no** form of this command to restore the default setting.

dot1x default-user-limit *num*

no dot1x default-user-limit

Parameter Description	Parameter	Description
	num	The maximum auth-user number allowed by a controlled interface, in the range from 1 to 1,000,000

Defaults By default, no limit is set for the auth-user number.

Command mode Interface configuration mode

Usage Guide This command is used to limit the number of users to be authenticated on a specific port.

Configuration Examples The following example sets the maximum auth-user number on a controlled interface.

```
Hostname(config-if)# dot1x default-user-limit 10
```

Related Commands

Command	Description
show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1X interface.
show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1X interface.

Platform Description N/A

4.24 dot1x dynamic-vlan enable

Use this command to enable dynamic VLAN.

Use the **no** form of this command to disable the function.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Dynamic VLAN is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to assign VLANs to authenticated users dynamically.

Configuration Examples The following example enables dynamic VLAN.

```
Hostname(config-if)# dot1x dynamic-vlan enable
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description N/A

4.25 dot1x guest-vlan

Use this command to configure the guest VLAN for port-control.
Use the **no** form of the command to disable the function.
dot1x guest-vlan
no dot1x guest-vlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults The guest VLAN is not configured by default.

Command Mode Interface configuration mode

Usage Guide Before using guest VLAN, you need to execute **dot1x dynamic-vlan enable** command first, or the configured guest VLAN does not take effect.
When configuring guest VLAN, it is recommended not to modify L2 attribute of the port, especially not to add the port to a VLAN manually.

Configuration Examples The following example configures VLAN 20 as 802.1X guest VLAN.

```
Hostname(config-if)# dot1x guest-vlan 20
```

Related Commands

Command	Description
show running-config	Displays the 802.1X configuration.

Platform Description N/A

4.26 dot1x mac-auth-bypass

Use this command to configure single MAB authentication.
Use the **no** form of this command to restore the default setting.
dot1x mac-auth-bypass
no dot1x mac-auth-bypass

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command on a single dumb terminal.

Configuration Examples The following example configures single MAB authentication.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
```

Related Commands	Command	Description
	show dot1x port-control interface	Displays the information about 802.1X on the interface.

Platform Description N/A

4.27 dot1x mac-auth-bypass multi-user

Use this command to configure multiple MAB authentications.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command when the interface is connected with multiple dumb terminals.

Configuration Examples The following example configures multiple MAB authentications.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.28 dot1x mac-auth-bypass timeout-activity

Use this command to set the MAB authentication timeout interval.

dot1x mac-auth-bypass timeout-activity *time*

no dot1x mac-auth-bypass timeout-activity

Parameter Description

Parameter	Description
time	The online time, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 0 second.

Command Mode Interface configuration mode

Usage Guide Use this command to set the MAB authentication timeout interval for dumb terminals.

Configuration Examples The following example sets the MAB authentication timeout interval.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
timeout-activity 3600
```

Related Commands

Command	Description
show dot1x port-control interface	Displays the 802.1X information.
show dot1x port-control interface	Displays the 802.1X information.

Platform Description N/A

4.29 dot1x mac-auth-bypass violation

Use this command to configure the MAB violation.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to configure the MAB violation on the port with only one dumb terminal in single MAB environment.

Configuration Examples The following example configures the MAB violation.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass violation
```

Related Commands	Command	Description
	show dot1x port-control interface	Displays the 802.1X information.

Platform Description N/A

4.30 dot1x mac-auth-bypass vlan

Use this command to configure the MAB VLAN function.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass vlan *vlan-list*

no dot1x mac-auth-bypass vlan *vlan-list*

Parameter Description	Parameter	Description
	vlan-list	Configures the MAB VLANs.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to allow users within specified VLANs on the port to perform MAB authentication.

Configuration Examples The following example configures MAB VLANs.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5, 8-20
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.31 dot1x max-req

Use this command to set the maximum attempts of authentication requests.

dot1x max-req *num*

Parameter Description	Parameter	Description
	num	Maximum attempts

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples The following example sets the maximum attempts of authentication requests to 2.

```
Hostname(config)# dot1x max-req 2
```

Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.

Platform Description N/A

4.32 dot1x multi-account enable

Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.

Use the **no** form of this command to restore the default setting.

dot1x multi-account enable

no dot1x multi-account enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use the command to enable the multiple-account authentication if you want to switch the username in the authentication or re-authentication, especially in the windows domain authentication.

Configuration Examples The following example enables the multiple-account authentication.

```
Hostname(config)# dot1x multi-account enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.33 dot1x multi-mab quiet-period

Use this command to set the quiet time after the multiple MAB authentication failure.

dot1x multi-mab quiet-period *time*

Parameter Description	Parameter	Description
	time	Sets the quiet period after the multiple MAB authentication failure, in the range from 0 to 65,535 in the unit of seconds.

Defaults The default is 0 second, indicating no quiet period.

Command Mode Global configuration mode

Usage Guide The default setting is recommended.

Configuration Examples The following example sets the quiet period after the multiple MAB authentication failure to 2 seconds.

```
Hostname(config)# dot1x multi-mab quiet-period 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.34 dot1x multi-mab quiet-user authen-num

Use this command to set the rate of initiating authentication using the MAC address in a blocked multi-user MAB user entry. Use the **no** form of this command to restore the default settings.

dot1x multi-mab quiet-user authen-num [*authen-num*]

no dot1x multi-mab quiet-user authen-num

Parameter	Parameter	Description

Description		
	authen-num	Sets the rate of initiating authentication using the MAC address in a blocked multi-user MAB user entry, in the number of MAC addresses per second. The value range is from 1 to 1000.

Defaults The default rate of initiating authentication using the MAC address in a blocked multi-user MAB user entry is 50 MAC addresses per second.

Command Mode Global configuration mode

Default Level 14

Usage Guide The default setting is recommended.

Configuration Examples The following example sets the rate of initiating authentication using the MAC address in a blocked multi-user MAB user entry to 3 MAC addresses per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user authen-num 3
```

Prompt Messages N/A

Platform Description N/A

4.35 dot1x multi-mab quiet-user fail-times

Use this command to set the number of authentication failures required for aging a user. Use the **no** form of this command to restore the default settings.

dot1x multi-mab quiet-user fail-times [*fail-times*]

no dot1x multi-mab quiet-user fail-times

Parameter Description	Parameter	Description
	fail-times	Sets the number of authentication failures required for aging a user. The value range is from 1 to 65,535.

Defaults The default number of authentication failures required for aging a user is 60.

Command Mode Global configuration mode

Default Level 14

Usage Guide A user who fails the authentication is required to be aged. This command is used to configure the aging rule for the user failing the authentication.

Configuration Examples The following example sets the number of MAB authentication failures required for aging a user to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user fail-times 3
```

Prompt Messages N/A

Platform Description N/A

4.36 dot1x multi-mab quiet-user reject-times

Use this command to set the number of server rejections required for deleting a blocked user entry. Use the **no** form of this command to restore the default settings.

dot1x multi-mab quiet-user reject-times [*reject-times*]

no dot1x multi-mab quiet-user reject-times

Parameter Description

Parameter	Description
reject-times	Sets the number of server rejections required for deleting a blocked user entry.

Defaults The default number of server rejections required for deleting a blocked user entry is 1.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example sets the number of server rejections required for deleting a blocked user entry to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user reject-times 3
```

Prompt Messages N/A

Platform N/A

Description

4.37 dot1x not-private-supplicant compatible

Use this command to enable the compatibility with third-party supplicants. Use the **no** form of this command to restore the default settings.

dot1x not-private-supplicant compatible

no dot1x not-private-supplicant compatible

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After this function is enabled, the device can receive TLV-encoded reply msg packets sent by third-party supplicants. In the packets, the type field is of 1 byte and has a fixed value of 09; the length field occupies 1 byte; the value field refers to the character string.

Configuration Examples The following example enables the compatibility with third-party supplicants.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x not-private-supplicant compatible
```

Prompt Messages N/A

Platform Description N/A

4.38 dot1x port-control auto

Use this command to configure the 802.1X authentication on the port.

Use the **no** form of this command to restore the default setting.

dot1x port-control auto

no dot1x port-control

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples The following example configures the 802.1X authentication on the port.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x port-control auto
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.39 dot1x port-control-mode

By default, 802.1x adopts MAC address-based control mode. In this mode, only authenticated users have access to the network, while other users that connect to the same port cannot access the network. In the port-based control mode, however, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all the users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user who is enabled to use the network normally. If you find other users on the port, you should clear all the users on the port and re-authenticate. The authentication mode can be configured using the following commands

dot1x port-control-mode { mac-based | port-based }

no dot1x port-control-mode

Parameter Description	Parameter	Description
	mac-based	Enable the MAC address-based control.
	port-based	Enable port-based control.
	port-based single-host	Enable single host-based control.

Defaults MAC address-based access control is used by default.

Command Mode Interface configuration mode.

Usage Guide Use the **show dot1x port-control** command to show the 802.1X configuration for the port. Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display

port-based and use **show running-config** to display dot1x port-control-mode port-based single-host. Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

Configuration Examples The following example sets the port to participate in authentication and enable port-based authentication.

```
Hostname(config-if-GigabitEthernet 0/0)# dot1x port-control-mode port-based
```

Related Commands

Command	Description
show dot1x port-control	Displays the port control mode.
show running-config	Displays the configuration.

Platform Description N/A

4.40 dot1x private-supplicant-only

Use this command to filter clients except our company's clients.

Use the **no** form of this command to restore the default setting.

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used for authentication supporting only our company's clients.

Configuration Examples The following example filters clients except our company's clients.

```
Hostname(config)# dot1x private-supplicant-only
```

Related Commands

Command	Description
show dot1x private-supplicant-only	Displays the information about the private supplicant.

Platform Description N/A

4.41 dot1x probe-timer alive

Use this command to set the terminal alive interval.

dot1x probe-timer alive *time*

Parameter Description	**Parameter**	**Description**
	time	Terminal alive interval, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 250 seconds.

Command Mode Global configuration mode

Usage Guide If the device does not receive the probe packet from the terminal when the terminal alive interval expires, the device is considered offline. The default setting is recommended.

Configuration Examples The following example sets terminal alive interval to 120 seconds.

```
Hostname(config)# dot1x probe-timer alive 120
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.42 dot1x probe-timer interval

Use this command to set terminal detection interval.

dot1x probe-timer interval *time*

Parameter Description	**Parameter**	**Description**
	time	Terminal detection interval in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 20 seconds.

Command Mode Global configuration mode

Usage Guide The default setting is recommended.

Configuration The following example sets terminal detection interval to 30 seconds.

Examples

```
Hostname(config)# dot1x probe-timer interval 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.43 dot1x pseudo source-mac

Use this command to use a virtual MAC address as the source MAC address of the 802.1X packets sent by the device.

Use the **no** form of this command to disable the usage of a virtual MAC address as the source MAC address of the 802.1X packets sent by the device.

dot1x pseudo source-mac

no dot1x pseudo source-mac

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide By default, the device uses its own MAC address as the source MAC address of the EAP packets for the 802.1X authentication. Some versions of our company's supplicant judge whether the access device is our company's device based on the source MAC address of the EAP packets. If the access device is our company's device, the supplicant device performs some private features. Configure this command if you want to enable these features.

Configuration Examples The following example uses the virtual MAC address as the source MAC address of the 802.1X packets sent by the device:

```
Hostname(config)# dot1x pseudo source-mac
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.44 dot1x re-authentication

Use this command to enable timed re-authentication function.

Use the **no** form of the command to restore the default setting.

dot1x re-authentication

no dot1x re-authentication

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command will re-authenticate the supplicant periodically after he passes the authentication. Use the **show dot1x** command to display 802.1X configuration. The default setting is recommended.

Configuration Examples The following example enables timed re-authentication function.

```
Hostname(config)# dot1x re-authentication
```

Related Commands	**Command**	**Description**
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.45 dot1x reauth-max

Use this command to set the maximum re-auth attempts.

Use the **no** form of this command to restore the default setting.

dot1x reauth-max *num*

no dot1x reauth-max

Parameter Description	**Parameter**	**Description**
	num,	Maximum re-auth attempts. The range is from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use this command to specify the maximum number of supplicant re-authentications. Use the **show dot1x** command to display 802.1X configuration.

Configuration Examples The following example sets the maximum re-auth attempts to 2.

```
Hostname(config)# dot1x reauth-max 2
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.46 dot1x redirect

Use this command to enable the second generation SU upgrade function.

Use the **no** form of this command to restore the default setting.

dot1x redirect

no dot1x redirect

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Redirect to the supplicant software download website through the browser. See *Web Authentication Configuration Guide* for details about parameters.

Configuration Examples The following example enables the second generation SU upgrade function,

```
Hostname(config)# dot1x redirect
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.47 dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default.

Use this command to prevent users from transition.

Use the **no** form of this command to restore the default setting.

dot1x stationarity enable

no dot1x stationarity enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.

Configuration Examples The following example prevents the user from transiting from 802.1X port to other port.

```
Hostname(config)# dot1x stationarity enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.48 dot1x timeout quiet-period

Use this command to set the quiet period after authentication failure.

Use the **no** form of this command to restore the default setting.

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter Description

Parameter	Description
time	Sets the quiet period after authentication failure, in the range from 1 to 65,535 in the unit of seconds.

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide When authentication fails, the supplicant must wait for a period of time before re-authentication.

Configuration Examples The following example sets the quiet period after authentication failure to 60 seconds.

```
Hostname(config)# dot1x timeout quiet-period 60
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description N/A

4.49 dot1x timeout re-authperiod

Use this command to set the re-authentication interval when re-authentication is enabled.

dot1x timeout re-authperiod *time*

Parameter Description

Parameter	Description
time	Authentication interval, in the range from 0 to 65,535 in the unit of seconds.

Defaults The default is 3,600 seconds.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples The following example sets the re-authentication interval to 2,400 seconds.

```
Hostname(config)# dot1x timeout re-authperiod 2400
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description N/A

4.50 dot1x timeout server-timeout

Use this command to set the server timeout interval.

dot1x timeout server-timeout *time*

Parameter Description

Parameter	Description
time	The server timeout interval, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide By default, the timeout of the 802.1X server is less than that of the Radius server. Use this command to raise the 802.1X timeout so as to exceed the Radius value. For details, see *Configuration Guide*.

Configuration Examples The following example set the server timeout interval to 10 seconds.

```
Hostname(config)# dot1x timeout server-timeout 10
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description N/A

4.51 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant.
Use the **no** form of this command to restore the default setting.
dot1x timeout supp-timeout *time*
no dot1x timeout supp-timeout

Parameter Description

Parameter	Description
time	Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.

Defaults The default is 3 seconds.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to show display 802.1X configuration.

Configuration Examples The following example sets the authentication timeout between the device and the supplicant to 10s:

```
Hostname(config)# dot1x timeout supp-timeout 10
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1x.

Platform N/A

Description

4.52 dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval.

dot1x timeout tx-period *time*

Parameter Description

Parameter	Description
time	The request/id packet re-transmission interval, in range from 1 to 65,535 in the unit of seconds

Defaults The default is 3 seconds.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to display 802.1X configuration.

Configuration Examples The following example sets the request/id packet re-transmission interval to 5 seconds.

```
Hostname(config)# dot1x timeout tx-period 5
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description N/A

4.53 dot1x user-name compatible

Use this command to configure the compatibility function for H3C 802.1X authentication clients and authentication servers.

Use the **no** form of this command to restore the default setting.

dot1x user-name compatible

no dot1x user-name compatible

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Enable this function when the H3C authentication client and authentication server are used for 802.1X authentication or the H3C authentication server is used for MAB authentication.

Configuration Examples The following example configures the compatibility function for H3C 802.1X authentication clients and authentication servers.

```
Hostname(config)# dot1x user-name compatible
```

Platform Description N/A

4.54 dot1x valid-ip-acct enable

Use this command to enable IP address-triggered accounting.

Use the **no** form of this command to restore the default setting.

dot1x valid-ip-acct enable

no dot1x valid-ip-acct enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable accounting only when users obtain valid IP addresses.

Configuration Examples The following example enables IP address-triggered accounting.

```
Hostname(config)#dot1x valid-ip-acct enable
```

Platform Description N/A

4.55 dot1x valid-ip-acct timeout

Use this command to configure IP address-triggered accounting timeout.

Use the **no** form of this command to restore the default setting.

dot1x valid-ip-acct timeout *time*

no dot1x valid-ip-acct timeout

Parameter Description

Parameter	Description

time	IP address-triggered accounting timeout in the unit of minutes

Defaults The default is 5 minutes.

Command Mode Global configuration mode

Usage Guide The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.

Configuration Examples The following example configures IP address-triggered accounting timeout.

```
Hostname(config)# dot1x valid-ip-acct timeout 10
```

Platform Description N/A

4.56 dot1x system disable

Use this command to disable global 802.1x. Use the **no** form of this command to restore the default settings.

dot1x system disable

no dot1x system disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, global 802.1x is enabled.

Command Mode Global configuration mode

Usage Guide (Optional) When the server is unreachable, disable global 802.1x, so users can access the Internet without authentication. After the server resumes reachability, enable global 802.1x, and users have to pass authentication before accessing the Internet.

Configuration Examples The following example disables global 802.1x.

```
Hostname(config)# dot1x system disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is only supported on switches.

4.57 show dot1x

Use this command to display the 802.1X setting.

show dot1x

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the 802.1X setting.

```
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
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.

dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.58 show dot1x auth-address-table

Use this command to display 802.1X authentication address table.

show dot1x auth-address-table [**address** *addr* | **interface** *interface*]

Parameter Description

Parameter	Description
addr	Physical IP address that can be authenticated
interface	Interface number

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the 802.1X authentication address table.

```
Hostname #show dot1x auth-address-table
Interface       Address
---------------- -------------------
Fa0/1          00d0.f800.0c0e
Fa0/2          001a.c800.0102

Hostname #show dot1x auth-address-table interface fastEthernet 0/1
Interface       Address
---------------- -------------------
Fa0/1          00d0.f800.0c0e

Hostname #show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface       Address
---------------- -------------------
```

```
Fa0/1          00d0.f800.0c0e
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1x authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.59 show dot1x auto-req

Use this command to display the auto-request authentication information.

show dot1x auto-req

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the auto-request authentication information.

```
Hostname# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
```

Related

Command	Description

Commands		
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.60 show dot1x max-req

Use this command to display the maximum number of request/challenge packet transmission.

show dot1x max-req

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the maximum number of request/challenge packet transmission.

```
Hostname#show dot1x max-req

Max-Req: 3 Times
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.

dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.61 show dot1x port-control

Use this command to display the port-control information.

show dot1x port-control [**interface** *interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type
interface-number	Interface ID

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the port-control information.

```
Hostname#show dot1x port-control
Interface Mode      Dynamic-User Static-User Max-User  Authened MAB
--------- ---------- ------------ ----------- --------- -------- ---------
Gi0/5    mac-based  0           0          unlimited no      disable
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant

	re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.62 show dot1x private-supplicant-only

Use this command to display the information about the private supplicant.

show dot1x private-supplicant-only

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information about the private supplicant:

```
Hostname#show dot1x private-supplicant-only

private-supplicant-only: Disabled
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.

dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.63 show dot1x probe-timer

Use this command to display the configuration of online user probe.

show dot1x probe-timer

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of online user probe.

```
Hostname#show dot1x probe-timer
Hello Interval   : 20
Hello Alive      : 60
```

Field Description

Command	Description
Hello Interval	Sets the probe period.
Hello Alive	Sets the probe alive interval.

Related Commands

Command	Description
N/A	N/A.

Platform Description N/A

4.64 show dot1x re-authentication

Use this command to display re-authentication status.

show dot1x re-authentication

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays re-authentication status.

```
Hostname#show dot1x re-authentication


Reauth-Enabled: Disabled
```

Command	Description
Reauth-Enabled	Whether to enable re-authentication.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.65 show dot1x reauth-max

Use this command to display the maximum re-auth attempts.

show dot1x reauth-max

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the maximum re-authentication attempts.

```
Hostname#show dot1x reauth-max


Reauth-Max: 3 Times
```

Command	Description
Reauth-Enabled	Sets the maximum re-authentication attempts.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.66 show dot1x summary

Use this command to display the 802.1X authentication summary.

show dot1x summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide It is convenient to display the 802.1X authentication summary according to the MAC address or username.

Configuration Examples The following example displays the summary of 802.1X authentication.

```
Hostname#show dot1x summary
ID      User      MAC           Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
-------- ---------- --------------  --------- ---- ---------- ---------------
------------- ----------- --------- ------------------
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions**.**
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.

dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description N/A

4.67 show dot1x timeout quiet-period

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

show dot1x timeout quiet-period

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

Configuration Examples The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.

```
Hostname#show dot1x timeout quiet-period


Quiet-Period: 10 Seconds
```

Parameter Description:

Parameter	Description
Quiet-Period	The time for the device to wait before re-authentication after the authentication failure.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.68 show dot1x timeout re-authperiod

Use this command to display the re-authentication interval.

show dot1x timeout re-authperiod

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the re-authentication interval.

Configuration Examples The following example displays the re-authentication interval.:

```
Hostname#show dot1x timeout re-authperiod

Reauth-Period: 3600 Seconds
```

Parameter Description:

Parameter	**Description**
Reauth-Period	Re-authentication interval.

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.69 show dot1x timeout server-timeout

Use this command to display the authentication timeout period.

show dot1x timeout server-timeout

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the authentication timeout period.

Configuration Examples Use this command to display the authentication timeout period:

```
Hostname#show dot1x timeout server-timeout


Server-Timeout: 5 Seconds
```

Parameter Description:

Parameter	Description
Server-Period	AuthenticationServer timeout periodinterval.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.70 show dot1x timeout supp-timeout

Use this command to display the request/challenge packets re-transmission interval.

show dot1x timeout supp-timeout

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/challenge packets re-transmission interval.

Configuration Examples Use this command to display the request/challenge packets re-transmission interval:

```
Hostname#show dot1x timeout supp-timeout


Supp-Timeout: 3 Seconds
```

Field Description:

Field	Description
Server-Period	The request/challenge packets re-transmission interval.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

4.71 show dot1x timeout tx-period

Use this command to display the request/id packets re-transmission interval.

show dot1x timeout tx-period

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/id packets re-transmission interval.

Configuration Examples Use this command to display the request/ id packets re-transmission interval:

```
Hostname#show dot1x timeout tx-period

Tx-Period: 30 Seconds
```

Parameter Description:

Parameter	**Description**
Tx-Period	Request/id packets re-transmission interval.

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.72 show dot1x user id

Use this command to display the information about 802.1X authentication users based on user IDs.

show dot1x user id *id*

Parameter Description	**Parameter**	**Description**
	id	User ID

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its ID.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user ID.

```
Hostname#show dot1x user id 16777225

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
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 :
Parameter Description:
```

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user accesses from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is our company's device
Start accounting	The accounting is enabled
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level
user acl-name	The ACL information

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

4.73 show dot1x user mac

Use this command to display the information about 802.1X authentication users based on MAC addresses.

show dot1x user mac *mac-addr*

Parameter Description	**Parameter**	**Description**
	mac-addr	MAC address

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user's MAC address.

```
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
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 :
```

Parameter Description:

Parameter	**Description**

User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is our company's device
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level
user acl-name	The ACL information

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.74 show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

show dot1x user name *name*

Parameter Description

Parameter	Description
name	User name

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user name.

```
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
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 :
```

Parameter Description:

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is our company's device.
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level.
user acl-name	The ACL information.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5 Web Authentication Commands

5.1 accounting

Use this command to set an accounting method for the template.
Use the **no** form of this command to restore the default setting.
accounting { *method-list* }
no accounting

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults N/A

Command Mode Template configuration mode

Usage Guide The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

Configuration Examples The following example sets the **mlist1** accounting method for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)# accounting mlist1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.2 authentication

Use this command to set an authentication method for the template.
Use the **no** form of this command to restore the default setting.
authentication { *method-list* }
no authentication

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults N/A

Command Mode Template configuration mode

Usage Guide The *method-list* parameter in this command should be consistent with the Web authentication method list configured in AAA.
The first generation authentication does not support the authentication method list configuration.

Configuration Examples The following example sets the **mlist1** authentication method for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)#authentication mlist1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 bindmode

Use this command to set a binding mode for the template.
Use the **no** form of this command to restore the default setting.
bindmode { **ip-mac-mode** | **ip-only-mode** }
no bindmode

Parameter Description

Parameter	Description
ip-mac-mode	IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry.
ip-only-mode	IP only mode. The device writes only the IP address information into the forwarding entry. On the L3 network, it is recommended to adopt this mode in case that the MAC address is inaccurate.

Defaults The default is **ip-mac-mode**.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples The following example adopts the IP only mode for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)# bindmode ip-only-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.4 clear web-auth direct host

Use this command to clear all authentication-exempted users.

clear web-auth direct-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all authentication-exempted users.

```
Hostname# clear web-auth direct-host
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

clear web-auth direct-site

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all authentication-exempted network resources.

```
Hostname# clear web-auth direct-site
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.6 clear web-auth user

Use this command to force the user to go offline.

clear web-auth user { **all** | **ip {** *ip-address* | *ipv6-address* } | **mac** *mac-address* **| name** *name-string* | **session-id** *num* }

Parameter Description

Parameter	Description
ip-address	Specifies the user's IPv4 address.
ipv6-address	Specifies the user's IPv6 address.
mac-address	Specifies the user's MAC address.
name-string	Specifies the user name.
num	Specifies the user's AAA session ID.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example forces all users to go offline.

```
Hostname(config) clear web-auth user all
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

5.7 fmt

Use this command to set the URL redirection format in the second template configuration mode.

fmt { cmcc-ext1 | cmcc-ext2 | cmcc-normal }

Parameter Description

Parameter	Description
cmcc-ext1	Extended CMCC format
cmcc-ext2	Liaoning CMCC format
cmcc-normal	Standard CMCC format

Defaults The default URL redirection format is our company's format.

Command Mode Template configuration mode

Usage Guide Use this command to set the URL redirection format based on the corresponding portal standard.

Configuration Examples The following example sets the URL redirection format to extended CMCC format.

```
Hostname(config.tmplt.eportalv2)#fmt cmcc-ext1
```

Platform Description N/A

5.8 http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP.

Use the **no** form of this command to restore the default setting.

http redirect direct-arp { *ip-address* [*ip-mask*] }

no http redirect direct- arp { *ip-address* [*ip-mask*] }

Parameter Description

Parameter	Description
ip-address	IPv4 address
ip-mask	(Optional) IPv4 mask

Defaults No authentication-exempted ARP resource is configured by default.

Command Mode Global configuration mode

Usage Guide The user cannot learn the ARPs of devices with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

Configuration Examples The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

```
Hostname(config)# http redirect direct-arp 172.16.0.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.9 http redirect direct-site

Use this command to set the range of authentication-exempted network resources.
Use the **no** form of this command to restore the default setting.
http redirect direct-site { *ipv6-address* | *ip-address* [*ip-mask*] [**arp**] }
no http redirect direct-site { *ipv6-address* | *ip-address* [*ip-mask*] }

Parameter Description

Parameter	Description
ipv6-address	IPv6 address of the authentication-exempted network resources
ip-address	IPv4 address of the authentication-exempted network resources
ip-mask	IPv4 address mask of the authentication-exempted network resources (optional)
arp	If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only.

Defaults No authentication-exempted network resource is set.

Command Mode Global configuration mode

Usage Guide When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites.
Up to 50 authentication-exempted users are supported.

Configuration Examples The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
Hostname(config)# http redirect direct-site 172.16.0.1
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.10 http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port.
Use the **no** form of this command to restore the default setting.
http redirect port *port-num*
no http redirect port *port-num*

Parameter Description

Parameter	Description
port-num	Destination port of the HTTP request

Defaults The default is port 80.

Command Mode Global configuration mode

Usage Guide When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.
By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.
This command is used to change the destination port of HTTP packets that are intercepted by the access device.
Up to 10 ports can be configured, excluding ports (80, 443).

Configuration Examples The following example redirects users' HTTP requests with port 8080.

```
Hostname(config)# http redirect port 8080
```

The following example does not redirect users' HTTP requests with port 80.

```
Hostname(config)# no http redirect port 80
```

Related Commands

Command	Description

show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.11 http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.

Use the **no** form of this command to restore the default setting.

http redirect session-limit *session-num* [**port** *port-session-num*]

no http redirect session-limit

Parameter Description

Parameter	Description
session-num	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
port-session-num	The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535.

Defaults Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

Command Mode Global configuration mode

Usage Guide To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.

In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

Configuration Examples The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4.

```
Hostname(config)# http redirect session-limit 4
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.12 http redirect timeout

Use this command to set the timeout for the redirection connection maintenance.

Use the **no** form of this command to restore the default setting.

http redirect timeout *seconds*

no http redirect timeout

Parameter Description

Parameter	Description
seconds	Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds.

Defaults The default is 3 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

Configuration Examples The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
Hostname(config)# http redirect timeout 4
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.13 ip

Use this command to set an IP address for the portal server.

Use the **no** form of this command to restore the default setting.

port { *ip-address* }

no port

Parameter Description

Parameter	Description
ip-address	The IPv4 address of the portal server

Defaults No IP address is set for the portal server by default.

Command Mode Template configuration mode

Usage Guide This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

Configuration Examples The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```
Hostname(config.tmplt.eportalv1)#ip 172.16.0.1
Hostname(config.tmplt.eportalv1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.14 ip portal source-interface

Use this command to specify a communication port for the portal server.

Use the **no** form of this command to restore the default setting.

ip portal source-interface *interface-type interface-num*

no ip portal source-interface

Parameter Description

Parameter	Description
interface-type	Port type
interface-num	Port No.

Defaults No communication interface is specified by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example specifies an aggregate port as the communication port.

```
Hostname (config)# ip portal source-interface Aggregateport 1
```

Platform Description N/A

5.15 port

Use this command to set a surveillance port for the portal server.

Use the **no** form of this command to restore the default setting.

port { *port-num* }

no port

Parameter Description

Parameter	Description
port-num	The surveillance port of the portal server, which is on only the 2nd generation portal server,

Defaults The default is 50100 based on the UDP protocol.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples The following example sets the surveillance port number of the eportalv2 server to 10000.

```
Hostname(config.tmplt.eportalv2)#port 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.16 show web-auth control

Use this command to display the authentication configuration.

show web-auth control

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the authentication configuration and statistics information on the interface.

```
Hostname(config)#show web-auth control
 Port                   Control  Server Name          Online User Count
 ------------------------ -------- --------------------- -----------------
 GigabitEthernet 0/1      On      <not configured>     0
Hostname(config)#
```

Field	Description
Port	Name of the authentication port.
Control	Displays whether the Web authentication is enabled on the port or not.
Server Name	The customized server name on the port. **<not configured>** indicates the server name has not been configured.
Online User Count	The number of online users on this port.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.17 show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

show web-auth direct-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide I N/A

Configuration Examples The following example displays the address range of the authentication-exempted ARP.

```
Hostname(config)#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
Hostname(config)#
```

Field	Description
Address	IPv4 address.
Mask	IPv4 mask.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.18 show web-auth direct-host

This command is used to display the Web authentication-exempted users.

show web-auth direct-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the Web authentication-exempted users.

```
Hostname# show web-auth direct-host
Direct hosts:
 Address           Mask             Port        ARP Binding
 ---------------- ---------------- ---------- ------------
 192.168.0.1     255.255.255.255   Fa0/2       On
 192.168.4.11     255.255.255.255   Fa0/10      On
 192.168.5.0     255.255.255.0     Fa0/16      Off
```

Field	Description
Address	IP address of the user free of authentication
Mask	IP address mask of the user free of authentication
Port	Access device port that is bound with the user's IP address
ARP Binding	Enable/Disable ARP binding

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.19 show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

show web-auth direct-site

Parameter Description

Parameter	Description
N/A	N/A

Defaults No network resource without authentication is set.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the range of the Web authentication-exempted network resources without authentication.

```
Hostname(config)#show web-auth direct-site
Direct sites:
  Address        Mask           ARP Binding
  ---------------  ---------------  -----------
  1.1.1.1        255.255.255.255 Off
  2.2.2.2        255.255.255.255 On
Hostname(config)#
```

Field	Description
Address	IP address.

Mask	IP mask.
ARP Binding	Displays whether the ARP binding function is enabled.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.20 show web-auth ip-mapping

Use this command to display the portal-client mapping rule.

show web-auth ip-mapping

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the portal-client mapping rule.

```
Hostname(config)#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
Hostname(config)#
```

Platform Description N/A

5.21 show web-auth parameter

Use this command to display the HTTP redirect configuration.

show web-auth parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the HTTP redirect configuration

```
Hostname# show web-auth parameter
  session-limit: 10
  timeout:        5
```

Field	Description
session-limit	Total number of HTTP sessions that are created by an unauthenticated user.
timeout	Timeout interval of the redirection connection.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.22 show web-auth portal-check

Use this command to display the portal-check configuration.

show web-auth portal-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the portal-check configuration.

```
Hostname#sh web portal-check
Check:        Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
Escape:       Enable
Nokick:       Disable
```

Platform Description N/A

5.23 show web-auth rdport

Use this command to display the TCP interception port.

show web-auth rdport

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the TCP interception port.

```
Hostname#show web-auth rdport
Rd-Port:
80 443
Hostname#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.24 show web-auth syslog ip

Use this command to display online and offline records about users.

show web-auth syslog ip *ip-address*

Parameter Description

Parameter	Description
Ip-address	A user's IP address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command cannot be used to save original data after hot backup.

Configuration Examples The following example displays online and offline records of users.

```
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
```

Field	Description
Index	The number of the record.

Time	Time when the record is made.
Behavior	Online or offline behavior.
MAC	The Mac address of a user.
Vid	The VLAN ID of a user.
Port	The user port.
Timeused	The time when a user gets online.
Flow UP	The uplink traffic of a user.
Flow down	The downlink traffic of a user.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.25 show web-auth template

Use this command to display the portal server configuration.

show web-auth template

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the portal server configuration.

Configuration Examples The following example displays the port server configuration.

```
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:
Hostname#
```

Field	Description
Name	Template name.
Url	Server homepage address.
Ip	Server IP address.
Type	Server type, including the first generation portal server v1, the second generation portal server v2 and the intra portal server intra.
Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Acctmlist	Accounting method list name, which is on only the second generation portal server
Authmlist	Authentication method list name. which is on only the second generation portal server

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.26 show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

show web-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the user.

mac-address	MAC address of the user.
name-string	User name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the global Web authentication configuration and statistics.

```
Hostname# show web-auth user all
Current user num :  4, online 2

Address          Online   Time Limit    Time Used    Status  Name
---------------- -------  ------------- -------------- -------- ---------
192.168.0.11    On      0d 01:00:00   0d 00:15:10    Active
192.168.0.13    On      0d 01:00:00   0d 00:00:59    Active   111
192.168.0.25    Off     0d 01:00:00   0d 00:00:59    Create
192.168.0.46    Off     0d 01:00:00   0d 01:00:00    Destroy  222

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
```

Field	Description
Address	IP address of the user
Mac	MAC address of the user
Port	Access device port connected to the user
Online	Whether the user is online
Time Limit	Available duration of the user. 0 means unlimited.
Time Used	Online duration of the user
Time Start	Time when the user passes authentication and gets online
Status	User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.27 url

Use this command to set the portal server URL.
Use the **no** form of this command to restore the default setting.
url *url-string*
no url

Parameter Description

Parameter	Description
url-string	Portal server URL, starting with **http://** or **https://**. The maximum length of this address is 255 bytes.

Defaults No portal server URL is set by default.

Command Mode Template configuration mode

Usage Guide This command takes place of the **http redirect homepage** [*url-string*] command, which is now hidden as a compatible command.,
If no URL is specified, the default URL in the **http://[ip-address]** format will be adopted, among which **ip-address** is the IP address of the server.

Configuration Examples The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

```
Hostname(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.28 web-auth dhcp-check

Use this command to enable DHCP IP address check.
Use **no** form of this command to restore the default setting.

web-auth dhcp-check
no web-auth dhcp-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults DHCP IP address check is disabled by default.

Command Mode Global configuration mode

Usage Guide Only users whose IP addresses are allocated by DHCP are allowed to take authentication.

Configuration Examples The following example enables DHCP IP address check.

```
Hostname (config)# web-auth dhcp-check
```

Platform Description N/A

5.29 web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range.
Use the **no** form of this command to restore the default setting.
web-auth direct-host { *ipv4-address* [i*p-mask*] [**arp**] | *ipv6-address*
no web-auth direct-host { *ip-address* [*ip-mask*] | *ipv6-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of authentication-exempted user
ipv6-address	IPv6 address of authentication-exempted user
ip-mask	Mask of the IPv4 address free of authentication (optional).
arp	If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only.

Defaults No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

Command Mode Global configuration mode

Usage Guide When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.

Up to 50 users can be set to be exempted from authentication.

Configuration Examples The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
Hostname(config)# web-auth direct-host 172.16.0.1
```

Related Commands

Command	Description
show web-auth direct-host	Displays the users free of Web authentication.

Platform Description N/A

5.30 web-auth enable

Use this command to enable the Web authentication function on a port. This command is compatible with the **web-auth port-control** command.

Use the **no** form of this command to restore the default setting.

web-auth enable [**eportalv1 | eportalv2 |** *template-name*]

no web-auth enable

Parameter Description

Parameter	Description
eportalv1	Applies the first generation authentication template.
eportalv2	Applies the second generation authentication template.
template-name	Customized template.

Defaults The Web authentication function is disabled on the port by default.

The **default** template is eportalv1.

Command Mode Interface configuration mode

Usage Guide To ensure the Web authentication function, the authentication page URL should be configured. Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.

Configuration Examples The following example enables the Web authentication function on gigabitEthernet 0/14.

```
Hostname(config)# interface GigabitEthernet 0/14
Hostname(config-if-GigabitEthernet 0/14)# web-auth enable
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

5.31 web-auth linkdown-timeout

Use this command to set the link-down timeout.

Use the **no** form of this command to restore the default setting.

web-auth linkdown-timeout { *timeout* }

no web-auth linkdown-timeout

Parameter Description	Parameter	Description
	timeout	Link-down timeout

Defaults By default, the timeout is 60 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the link-down timeout to 30 seconds.

```
Hostname (config)# web-auth linkdown-timeout 30
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.32 web-auth logging enable

Use this command to enable the Web authentication syslog function.

Use the **no** form of this command to restore the default setting.

web-auth logging enable { *num* }

no web-auth logging enable

Parameter Description	Parameter	Description

num	The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to limit the syslog printing rate for only the functional module.

Configuration Examples The following example enables the syslog printing with no rate limit.

```
Hostname(config)# web-auth logging enable 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.33 web-auth portal key

Use this command to set the communication key between the access device and the authentication server.
Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.
web-auth portal key *key-string*
no web-auth portal key

Parameter Description

Parameter	Description
key-string	Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes.

Defaults No key is set by default.

Command Mode Global configuration mode

Usage Guide To use the Web authentication function, the communication key between the access device and the authentication server must be set.

Configuration The following example sets the communication key between the access device and the

Examples authentication server to web-auth.

```
Hostname(config)# web-auth portal key web-auth
```

Related Commands

Command	Description
http redirect	Sets the IP address of the authentication server.
http redirect homepage	Sets the address of the authentication homepage.
web-auth port-control	Enables the Web authentication on the port.

Platform Description N/A

5.34 web-auth portal-check

Use this command to enable portal server check.

Use the **no** form of this command to restore the default setting.

web-auth portal-check [**interval** *intsec*] [**timeout** *tosec*] [**retransmit** *retires*]

no web-auth porta-check

Parameter Description

Parameter	Description
Intsec	Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds.
tosec	Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds.
retries	Retry count in the range from 1 to 100. The default is 3.

Defaults Portal server check is disabled by default.

Command Mode Global configuration mode

Usage Guide It is recommended to use this command when there are multiple servers.

Configuration Examples The following example enables portal server check.

```
Hostname (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Platform Description N/A

5.35 web-auth portal-escape

Use this command to enable portal-escape function.
Use the **no** form of this command to restore the default setting.
web-auth portal-escape
no web-auth portal-escape

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command together with **web-auth portal-check** command to sustain key services when the portal server is abnormal.

Configuration Examples The following example enables portal-escape function.

```
Hostname (config)# web-auth portal-escape
```

Platform Description N/A

5.36 web-auth template

Use this command to create the first generation authentication template and enter its configuration mode.
web-auth template eportalv1

Use this command to create the second generation authentication template and enter its configuration mode.
web-auth template eportalv2

Use this command to create the customized second generation authentication template and enter its configuration mode.
web-auth template { *template-name* } **v2**

Use this command to remove the template.
no web-auth template { *template-name* }

Parameter Description

Parameter	Description
eportalv1	Applies the first generation authentication template.
eportalv2	Applies the second generation authentication template.
template-name	Sets the name of the customized authentication template.

Defaults No template is configured by default.

Command Mode Global configuration mode

Usage Guide You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands**.** The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command.

The original command **portal-server** is compatible on the device, which will be converted to this command.

To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ip-address]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

Configuration Examples The following example configures the **eportalv1** template.

```
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.37 web-auth update-interval

Use this command to set the interval at which the online user information is updated.

Use the **no** form of this command to restore the default setting.

web-auth update-interval {*seconds*}

no web-auth update-interval

Parameter

Parameter	Description

Description

seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.

Defaults The default is 180 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the interval at which the online user information is updated to 60 seconds.

```
Hostname(config)# web-auth update-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.38 web-auth vlan-control

Use this command to configure the authenticable VLAN list.

Use the **no** form of this command to restore the default setting.

web-auth vlan-control *vlan-list*

no web-auth vlan-control

Parameter Description

Parameter	Description
vlan-list	Authenticable VLAN list

Defaults The default is port-control authentication.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples Use this command to configure the authenticable VLAN list.

```
Hostname (config-if-GigabitEthernet 0/1)# web-auth vlan-control 1
```

Platform Description	N/A

6 SCC Commands

6.1 Identifier Description

The following is a list of command identifiers used in commands for reference:

Identifier	Description
vlanlist	Authentication-exemption VLAN list
interval	Authenticated-user online-status detection interval
thredshold	The traffic threshold of authenticated-user online-status detection

6.2 direct-vlan

Use this command to configure authentication-exemption VLANs.
direct-vlan *vlanlist*

Use this command to delete the authentication-exemption VLAN configuration.
no direct-vlan *vlanlist*

Parameter Description

Parameter	Description
vlanlist	VLAN list, which can be a VLAN or a group of VLANs.

Defaults By default, no authentication-exemption VLANs are configured.

Command Mode Global configuration mode

Default Level 14

Usage Guide You can use this command to configure authentication-exemption VLANs, so that users in specified VLANs can access the Internet without experiencing dot1x or Web authentication.

Configuration Examples The following example configures the VLAN2 as an authentication-exemption VLAN.

```
Hostname(config)# direct-vlan 2
```

Verification Use the **show direct-vlan** command to display the authentication-exemption VLAN configuration.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.3 nac-author-user maxinum

Use this command to configure the limit on IPv4 user capacity on a port.
nac-author-user maxinum *max-user-num*

Use this command to remove the limit on the IPv4 user capacity on a port.
no nac-author-user maxinum

Parameter Description

Parameter	Description
max-user-num	Defines the maximum number of IPv4 access users. The range is from 1 to 1,024.

Defaults By default, the number of IPv4 access users is not limited.

Command Mode Interface configuration mode

Default Level 14

Usage Guide Use this command to configure the maximum number of IPv4 access users on a port.

Configuration Examples The following example restricts the maximum number of IPv4 users to 100 on interface Gi 0/1.

```
Hostname(config)#int gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#nac-author-user maxinum 100
```

Verification 1. Use the **show nac-author-user** command to display the current and the maximum numbers of IPv4 access users on all ports.
2. Use the **show nac-author-user interface** *interface-name* command to display the current and the maximum numbers of IPv4 access users on the specified port.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.4 offline-detect interval threshold

Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval.
offline-detect interval *interval* **threshold** *thredshold*

Use this command to restore the default user online-status detection configuration.
default offline-detect

Use this command to disable user online-status detection.
no offline-detect

Parameter Description

Parameter	Description
interval	Indicates the interval of traffic detection (in minutes). The range is from 6 to 65,535 in minutes.
threshold	Indicates the traffic threshold (in bytes). The range is from 0 to 4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected.

Defaults By default, the detection interval is 8 hours and the traffic threshold is 0.

Command Mode Global configuration mode

Default Level 14

Usage Guide You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.

Configuration Examples The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes.

```
Hostname(config)#offline-detect interval 5 threshold 5120
```

Verification Use the **show running** command to display the configuration of online-status detection for authenticated users.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.5 show direct-vlan

Use this command to display the authentication-exemption VLAN configuration.

show direct-vlan

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide N/A

Configuration Examples The following example displays the authentication-exemption VLAN configuration.

```
Hostname #show direct-vlan
direct-vlan 5,7,100
```

Prompt Messages N/A

Platforms This command is supported only on switches.

6.6 show nac-author-user interface

Use this command to display the capacity limit and current number of IPv4 users on all interfaces or a specified interface.

show nac-author-user [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Command Mode Privileged EXEC mode

Level 14

Usage Guide N/A

Configuration The following example displays the current number and capacity limit of IPv4 users on interface Gi 0/1.

Examples

```
Hostname#show nac-author-user interface gi 0/1
 Port     Cur_num  Max_num
 --------  -------  -------
 Gi0/1    0        100
```

Prompt Messages N/A

Platforms N/A

6.7 station-move permit

Use this command to enable authenticated-user migration.
station-move permit

Use this command to disable authenticated-user migration.
no station-move permit

Parameter Description

Parameter	Description
N/A	N/A

Defaults Authenticated-user migration is not permitted by default.

Command Mode Global configuration mode

Level 14

Usage Guide You can enable the authenticated-user migration function to allow the online users to be authenticated again and get online from different physical locations (different ports or VLANs).

Configuration Examples The following examples enables authenticated-user migration.

```
Hostname(config)#station-move permit
```

Verification Use the **show running** command to check whether the authenticated-user migration function is enabled.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

7 Global IP-MAC Binding Commands

7.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

address-bind { *ip-address* | *ipv6-address* } mac-address

no address-bind { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address to be bound
ipv6-address	IPv6 address to be bound
mac-address	MAC address to be bound

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

```
The following example configures global IP-MAC address binding.Hostname#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Related Commands

Command	Description
show address-bind	Displays the IP address-MAC address binding table.

Platform Description N/A

7.2 address-bind binding-filter logging

Use this command to enable the logging filter. Use the **no** form of this command to restore the default setting.

address-bind binding-filter logging [**rate-limit** *rate*]

no address-bind binding-filter logging

Parameter

Parameter	Description

Description	**rate-limit *rate***	Printing rate of the logging filter of global IPv4 MAC binding. By default, the rate is 10 logs per minute. The configurable range is from 1 to 120 logs per minute.

Defaults Logging filter is disabled.

Command Mode Global configuration mode

Usage Guide By default, the rate is 10 logs per minute.
When a logging filter is configured, alert logs are printed if IP packets not containing matched IP address and MAC address are detected.
When a logging filter is configured, the number of non-printed logs is prompted if the actual printing rate exceeds the set rate.

Configuration Examples The following example enables logging filter:

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# address-bind binding-filter logging
Hostname(config)# end
```

Verification Run the **show running-config** command to display the configuration.

Platform Description N/A

7.3 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.
address-bind install
no address-bind install

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

Configuration Examples The following example enables a binding policy.

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# address-bind 3.3.3.3 00d0.f811.1112
Hostname(config)# address-bind install
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.4 address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

no address-bind ipv6-mode

Parameter Description	Parameter	Description
	compatible	Compatible mode
	loose	Loose mode
	strict	Strict mode

Defaults The default is strict mode.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the IPv6 address binding mode.

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# address-bind ipv6-mode compatible
```

Related Commands	Command	Description
	show address-bind uplink	Displays the exceptional port of the address binding.

Platform Description N/A

7.5 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

address-bind uplink *interface-id*

no address-bind uplink *interface-id*

Parameter Description

Parameter	Description
interface-id	Switching port or layer 2 aggregate port.

Defaults All ports are non-exception ports by default.

Command Mode Global configuration mode.

Usage Guide If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Configuration Examples

```
The following example configures the exception port. Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# address-bind uplink GigabitEthernet 0/1
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of address binding.

Platform Description N/A

7.6 show address-bind

Use this command to display global IP address-MAC address binding.

show address-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays global IPv4 address-MAC address binding.

```
Hostname#show address-bind
Total Bind Addresses in System : 1
IP Address        Binding MAC Addr
---------------    ----------------
192.168.5.1       00d0.f800.0001
```

Field	Description
Total Bind Addresses in System	IPv4 address-MAC address binding count
IP Address	Bound IP address
Binding MAC Addr	Bound MAC address

Related Commands

Command	Description
address-bind	Enables IP address-MAC address binding.

Platform Description N/A

7.7 show address-bind uplink

Use this command to display the exception port.

show address-bind uplink

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode N/A

Usage Guide N/A

Configuration Examples The following example displays the exception port.

```
Hostname#show address-bind uplink
Port      State
---------- ---------
Gi0/1     Enabled
Default    Disabled
```

Field	Description
Port	Short for exception ports. All ports are

	non-exception ports by default.
State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it it not.

Related Commands

Command	Description
address-bind uplink	Sets the exception port.

Platform Description N/A

8 Password-Policy Commands

8.1 password policy life-cycle

Use this command to set the password lifecycle. Use the **no** form of this command to restore the default setting.

password policy life-cycle days

no password policy life-cycle

Parameter Description

Parameter	Description
days	Sets the password lifecycle, in the range from 1 to 65535 in the unit of days.

Defaults No password lifecycle is set by default.

Command Mode Global configuration mode

Usage Guide This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the password lifecycle to 90 days.

```
Hostname(config)# password policy life-cycle 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

password policy min-size *length*

no password policy min-size

Parameter Description

Parameter	Description
length	Sets the minimum length of the password, in the range from 1 to 31.

Defaults No minimum length of the password is set by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used to set the minimum length of the password,

> This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the minimum length of the password to 8.

```
Hostname(config)# password policy min-size 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.

password policy no-repeat-times *times*

no password policy no-repeat-times

Parameter Description

Parameter	Description
times	The past several times when passwords are configured, in the range from 1 to 31.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this function is enabled, passwords used in the past several times are recorded. If the

new password has been used, the alarm message is displayed and password configuration fails.

This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples

The following example bans the use of passwords used in the past five times.

```
Hostname(config)# password policy no-repeat-times 5
```

Related Commands

Command	Description
N/A	N/A

8.4 password policy strong

Use this command to enable strong password check.

password policy strong

no password policy strong

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples

The following example configures the strong password check.

```
Hostname(config)# password policy strong
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.5 password policy forced-password-modify

Use this command to enable mandatory modification of weak passwords. Use the **no** form of this command to restore default setting.

password policy forced-password-modify

no password policy forced-password-modify

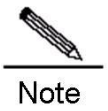
Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After mandatory modification of weak passwords is enabled, users have to change their passwords if the passwords are the same as corresponding accounts or contain characters or digits only.



After this command is executed, this function takes effect when the **enable password**, **enable secret**, and **username** *name* **password** *password* commands are run.

Configuration Examples The following example enables mandatory modifucation of weak passwords.

```
Hostname(config)# password policy forced-password-modify
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.6 password policy printable-character-check

Use this command to enable check for special characters in a password. Use the **no** form of this command to restore the default settings.

password policy printable-character-check

no password policy printable-character-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After strong password check and check for special characters in a password are configured, passwords that contain only special characters are invalid and cannot be configured successfully. There are 32 special characters in total, including 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 (/).

Configuration Examples The following example enables check for special characters in a password.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy strong
Hostname(config)# password policy printable-character-check
```

Verification Run the **show password policy** command to check whether check for special characters in a password is enabled.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

8.7 service password-encryption

Use this command to encrypt a password. Use the **no** form of this command to restore default setting.

service password-encryption

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration Examples The following example encrypts the password:

```
Hostname(config)# service password-encryption
```

Related Commands

Command	Description
enable password	Sets passwords of different privileges.

Platform Description N/A

8.8 show password policy

Use this command to display the password security policy set by the user.

show password policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the password security policy set by the user.

Configuration Examples The following example displays the password security policy set by the user.

```
Hostname#show password policy
Global password policy configurations:
 Password encryption:              Enabled
 Password strong-check:            Enabled
 Password min-size:                Enabled (6 characters)
 Password life-cycle:              Enabled (90 days)
 Password no-repeat-times:         Enabled (max history record: 5)
```

Field	Description
Password encryption	Whether to encrypt the password.
Password strong-check	Whether to enable password strong-check.
Password min-size	Whether to set the minimum length of the password.
Password life-cycle	Whether to set the password lifecycle.
Password no-repeat-times	

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9 Storm Control Commands

9.1 show storm-control

Use this command to display storm suppression information.

show storm-control [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Specifies an interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays storm control configuration on FastEthernet 0/1.

```
Hostname# show storm-control fastEthernet 0/1
Interface              Broadcast Control Multicast Control Unicast Control
Action
------------------------ ----------------- -----------------
--------------- --------
FastEthernet 0/1         1%              50%            1%     none
```

Related Commands

Command	Description
storm-control	Enables storm suppression.

Platform Description N/A

9.2 storm-control

Use this command to enable the storm suppression for unknown unicast packets.

Use the **no** or **default** form of this command to restore the default setting.

storm-control unicast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control unicast

default storm-control unicast

Use this command to enable the storm suppression for multicast packets.
Use the **no** or **default** form of this command to restore the default setting.
storm-control multicast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]
no storm-control multicast
default storm-control multicast

Use this command to enable the storm suppression for broadcast packets.
Use the **no** or **default** form of this command to restore the default setting.
storm-control broadcast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]
no storm-control broadcast
default storm-control broadcast

Parameter Description

Parameter	Description
level *percent*	Sets the bandwidth percentage, for example, 20 means 20%.
pps *packets*	Sets the pps, which means packets per second.
rate-bps	Rate allowed

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.
A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Configuration Examples The following example enables the multicast storm suppression on FastEthernet 0/1 and sets the allowed rate to 4M.

```
Hostname(config)# int fastEthernet 0/1
Hostname(config-if-FastEthernet 0/1)# storm-control multicast 4096
```

Related Commands

Command	Description
show storm-control	Displays storm suppression information.

Platform Description N/A

10 SSH Commands

10.1 crypto key generate

Use this command to generate a public key to the SSH server.

crypto key generate { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Generates an RSA key.
dsa	Generates a DSA key.

Defaults By default, the SSH server does not generate a public key.

Command Mode Global configuration mode

Usage Guide When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

- Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.
- RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.
- A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

Configuration Examples The following example generates an RSA key to the SSH server.

```
Hostname# configure terminal
Hostname(con fig)# crypto key generate rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key zeroize { **rsa** | **dsa** }	Deletes DSA and RSA keys and disables the SSH server function.

Platform Description N/A

10.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

crypto key zeroize { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Deletes the RSA key.
dsa	Deletes the DSA key.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

Configuration Examples The following example deletes a RSA key to the SSH server.

```
Hostname# configure terminal
Hostname(config)# crypto key zeroize rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key generate { **rsa	dsa** }	Generates DSA and RSA keys.

Platform Description N/A

10.3 disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [**vty**] *session-id*

Parameter Description

Parameter	Description
vty	Established VTY connection
session-id	ID of the established SSH connection, in the range from 0 to 35

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples The following example disconnects the established SSH connection by specifying the SSH session ID.

```
Hostname# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Hostname# disconnect ssh vty 1
```

Related Commands

Command	Description
show ssh	Displays the information about the established SSH connection.
clear line vty *line_number*	Disconnects the current VTY connection.

Platform Description N/A

10.4 disconnect ssh session

Use this command to disconnect the suspended SSH client session.

disconnect ssh-session *session-id*

Parameter Description

Parameter	Description
session-id	ID of the suspended SSH client session

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to disconnect the suspended SSH client session by specifying its session ID.

Configuration Examples The following example disconnects a SSH client session by specifying its session ID.

```
Hostname# disconnect ssh-session 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.5 ip scp server enable

Use this command to enable the SCP server function on a network device.

Use the **no** form of this command to restore the default setting.

ip scp server enable

no ip scp server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

Configuration Examples The following example enables the SCP server function.

```
Hostname# configure terminal
Hostname(config)# ip scp server enable
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.6 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter Description

Parameter	Description
retry times	Authentication retry times, ranging from 0 to 5

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

Configuration Examples The following example sets the authentication retry times to 2.

```
Hostname# configure terminal
Hostname(config)# ip ssh authentication-retries 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.7 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

Use the **no** form of this command to restore the default setting.

ip ssh cipher-mode { **cbc** | **ctr** | **others** }

no ip ssh cipher-mode

Parameter Description

Parameter	Description
cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC
ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
others	Encryption mode: Others Encryption algorithm: RC4

Defaults All encryption modes are supported by default.

Command Mode Global configuration mode

Usage Guide This command is used to set the SSH server encryption mode.

For theNetworks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

Configuration The following example enables CTR encryption mode.

Examples

```
Hostname# configure terminal
Hostname(config)# ip ssh cipher-mode ctr
```

Platform Description N/A

10.8 ip ssh compatible-ssh1x

Use this command to enable the SSHv1 function. Use the **no** form of this command to restore the default settings.

ip ssh compatible-ssh1x enable

no ip ssh compatible-ssh1x enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example enables the SSHv1 function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh compatible-ssh1x enable
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.9 ip ssh dh-exchange min-len

Use this command to configure the minimum length of the key generated by the key exchange algorithm of the SSH server. Use the **no** form of this command to restore the default settings.

ip ssh dh-exchange min-len { 1024 | 2048 }

no ip ssh dh-exchange min-len

Parameter Description

Parameter	Description
1024	Sets the minimum length of the key generated by the key exchange algorithm of the SSH server to 1024 bytes.
2048	Sets the minimum length of the key generated by the key exchange algorithm of the SSH server to 2048 bytes.

Defaults The default minimum length of the key generated by the key exchange algorithm of the SSH server is 2048 bytes.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example sets the minimum length of the key generated by the key exchange algorithm of the SSH server to 1024 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh dh-exchange min-len 1024
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.10 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.

Use the **no** form of this command to restore the default setting.

ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96 | sha2-256 | sha2-512**}

no ip ssh hmac-algorithm

Parameter Description

Parameter	Description
md5	MD5 algorithm
md5-96	MD5-96 algorithm
sha1	SHA1 algorithm
sha1-96	SHA1-96 algorithm
sha2-256	SHA2-256 algorithm
sha2-512	SHA2-512 algorithm

Defaults SSHv1: all the algorithms are not supported.
SSHv2: Six algorithms are supported. (MD5, SHA1, SHA1-96, MD5-96, SHA2-256 and SHA2-512 algorithms.)

Command Mode Global configuration mode

Usage Guide SSHv1 servers do not support algorithms for message authentication.
For our Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, SHA1-96, SHA2-256 and SHA2-512 algorithms. Set the algorithm on your demand.

Configuration Examples The following example sets the algorithm for message authentication to SHA1.

```
Hostname# configure terminal
Hostname(config)# ip ssh hmac-algorithm sha1
```

Platform Description N/A

10.11 ip ssh ip-block disable

Use this command to disable the IP address blocking function on the SSH server. Use the **no** form of this command to restore the default settings.

ip ssh ip-block disable

no ip ssh ip-block disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide When the number of authentication failures for logging to a device through SSH reaches the configured limit of IP address blocking, 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 period of blocked source IP address reaches the unblocking period requirement.

Configuration 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
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.12 ip ssh ip-block failed-times

Use this command to configure the number of authentication failures for blocking IP addresses and the time period for counting authentication failures on the SSH server. Use the **no** form of this command to restore the default settings.

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

Parameter	Description
failed-times	Configures the number of authentication failures for blocking IP addresses. The value range is from 1 to 10.
period-time	Configures the time period for counting authentication failures in minutes. The value range is from 1 to 120.

Defaults The default number of authentication failures for blocking IP addresses on the SSH server is 6 and the time period for counting authentication failures is 5 minutes.

Command Mode Global configuration mode

Default Level 14

Usage Guide 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 succeeds, the authentication failures are cleared.

Configuration Examples The following example sets the number of authentication failures for blocking IP addresses on the SSH server to 3 and the time period for counting authentication failures to 3 minutes.

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

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.13 ip ssh ip-block reactive

Use this command to configure the time period for awakening blocked IP addresses on the SSH server. Use the **no** form of this command to restore the default settings.

ip ssh ip-block reactive *reactive-interval*

no ip ssh ip-block reactive

Parameter Description

Parameter	Description
reactive-interval	Configures the time period for awakening blocked IP addresses in minutes. The value range is from 1 to 1000.

Defaults Blocked IP addresses are awakened every 5 minutes by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After the time period for awakening the blocked source IP address reaches the requirement, the entry with the blocked source IP address is cleared. An SSH client can use this IP address to log in to the device.

Configuration Examples The following example sets the time period for awakening blocked source IP addresses to 3 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh ip-block reactive 3
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.14 ip ssh key-exchange

Use this command to configure the Diffie–Hellman (DH) Algorithm supported by the SSH server. Use the **no** form of this command to restore the default settings.

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

Parameter	Description
dh_group_exchange_sha1	Sets the DH algorithm to diffie-hellman-group-exchange-sha1. The default key length is 2048 bytes and unconfigurable.
dh_group14_sha1	Sets the DH algorithm to diffie-hellman-group14-sha1. The key length is 2048 bytes.
dh_group1_sha1	Sets the DH algorithm to diffie-hellman-group1-sha1. The key length is 1024 bytes.
ecdh_sha2_nistp256	Sets the DH algorithm to ecdh_sha2_nistp256. The key length is 256 bytes.
ecdh_sha2_nistp384	Sets the DH algorithm to ecdh_sha2_nistp384. The key length is 384 bytes.
ecdh_sha2_nistp521	Sets the DH algorithm to ecdh_sha2_nistp521. The key length is 521 bytes.

Defaults By default, SSHv1 servers support no DH algorithm. SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256,

ecdh_sha2_nistp384, and ecdh_sha2_nistp521.

Command Mode Global configuration mode

Default Level 14

Usage Guide SSHv1 servers support no DH algorithm. SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521. You can select a DH algorithm supported by SSH servers as required.

Configuration Examples The following example sets the DH algorithm to diffie-hellman-group14-sha1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ssh key-exchange dh_group14_sha1
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

10.15 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

Use the **no** form of this command to restore the default setting.

ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

Parameter Description

Parameter	Description
username	User name
filename	Name of a public key file
rsa	The public key is a RSA key
dsa	The public key is a DSA key

Defaults N/A

Command Global configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example sets RSA and DSA key files associated with user **test**.

```
Hostname# configure terminal
Hostname(config)# ip ssh peer test public-key rsa flash:rsa.pub
Hostname(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.16 ip ssh port

Use this command to set a monitoring port ID for the SSH server.
ip ssh port *port*

Use either of the following commands to restore the monitoring port ID of the SSH server to the default value.
no ip ssh port
ip ssh port 22

Parameter Description

Parameter	Description
port	Monitoring port ID of the SSH server. The value ranges from 1025 to 65535.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example sets the monitoring port ID of the SSH server to 10000.

```
Hostname# configure terminal
Hostname(config)# ip ssh port 10000
```

Verification Run the **show ip ssh** command to display the configured monitoring port ID of the SSH server.

Prompts 1. If the required port ID is the same as the current value, a prompt is displayed, indicating that the current

port ID is the required value.

```
Hostname(config)# ip ssh port 22
% SSH tcp-port has been 22
```

2. If a port in the monitoring state is configured as the monitoring port of the SSH server, a prompt is displayed, indicating that the port is already in the monitoring state and you are required to set another port ID, and the SSH server still uses the previous port ID.

```
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)!
```

3. If a monitoring error occurs after a monitoring port ID is configured for the SSH server, a port ID configuration failure prompt is displayed.

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

4. If a port ID is configured successfully, a port ID configuration success prompt is displayed.

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

10.17 ip ssh source-interface

Use this command to specify a source interface for the SSH client. Use the **no** form of this command to remove the setting.

ip ssh source-interface *interface-name*

no ip ssh source-interface

Parameter Description

Parameter	Description
interface-name	Specifies a source interface for the SSH client, indicating that the SSH client takes the interface IP address as its source address.

Defaults The IP address of the interface that sends the SSH packet is taken as its source address by default.

Command Mode Global configuration mode

Usage Guide This command is used to specify the IP address of the specified interface as the source address of the SSH client.

Configuration Examples The following example specifies the IP address of interface Loopback 1 as the source address of the global SSH session.

```
Hostname(config)# ip ssh source-interface Loopback 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.18 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter Description	Parameter	Description
	time	Authentication timeout, in the range from 1 to 120 in the unit of seconds

Defaults The default is 120 seconds.

Command Mode Global configuration mode

Usage Guide The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

Configuration Examples The following example sets the timeout value to 100 seconds.

```
Hostname# configure terminal
Hostname(config)# ip ssh time-out 100
```

Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.19 ip ssh version

Use this command to set the version of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh version { **1** | **2** }

no ip ssh version

Parameter Description

Parameter	Description
1	Supports the SSH1 client connection request.
2	Supports the SSH2 client connection request.

Defaults SSH1 and SSH2 are compatible by default.

Command Mode Global configuration mode

Usage Guide This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

Configuration Examples The following example sets the version of the SSH server.

```
Hostname# configure terminal
Hostname(config)# ip ssh version 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.20 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

show crypto key mypubkey { **rsa | dsa | ecc** }

Parameter Description

Parameter	Description
rsa	Displays the RSA key.
dsa	Displays the DSA key.
ecc	Displays the ECC key.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

Configuration Examples The following example displays the information about the public key part of the public key to the SSH server.

```
Hostname(config)#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==
```

Related Commands

Command	Description
crypto key generate { **rsa** | **dsa** }	Generates DSA and RSA keys.

Platform Description N/A

10.21 show ip ssh

Use this command to display the information of the SSH server.

show ip ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide This command is used to display the information of the SSH server, including version, enablement state, authentication timeout, and authentication retry times.

Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH

version has been configured.

Configuration Examples The following example displays the information of the SSH server.

```
SSH and SCP disabled:
Hostname(config)#show ip ssh
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
Hostname(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

Related Commands

Command	Description
ip ssh version {**1** | **2**}	Configures the version for the SSH server.
ip ssh time-out time	Sets the authentication timeout for the SSH server.
ip ssh authentication-retries	Sets the authentication retry times for the SSH server.

Platform Description N/A

10.22 show ssh

Use this command to display the information about the established SSH connection.

show ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

Configuration The following example displays the information about the established SSH connection:

Examples

```
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
```

Field Description

Field	Description
Connection	VTY number
Version	SSH version
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compress algorithm
State	Connection state
Username	Username

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.23 show ssh session

Use this command to display the SSH Client session.

show ssh-session

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use this command to display the established SSH client session information, including the VTY number, SSH version, encryption algorithm, message authentication algorithm, connection state, and username.

Configuration Examples The following example display the established SSH client session.

```
Hostname#show ssh-session
Connect No.  SSH Version  Server Address
-----------  -----------  ---------------
0          2.0        192.168.23.122
```

```
1          1.5         192.168.23.122
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.24 ssh

Use this command to establish an encrypted session with a remote device.

ssh [**oob**] [**-v** { **1** | **2** }] [**-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*] { *ip-addr* | *hostname* } [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }] [**/vrf** *vrf-name*]

Parameter Description	Parameter	Description
	oob	Connects to the SSH server through out-of-band communication (generally through MGMT port), This parameter will be displayed only when the device has a MGMT port.
	-v	(Optional) The version of the SSH that is used to connect to the server, By default, it is SSHv2 ● Connect to the server via SSHv1. ● Connect to the server via SSHv2.
	-c { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }	(Optional) Specifies the encryption algorithm. The available encryption includes Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES), and Advantaged Encryption Standard (AES). Based on the length of the secret key, AES can be further divided into three types: aes128-cbc (128-bit secret key), aes192-cbc (192-bit secret key), and aes256-cbc (256-bit secret key) If no encryption algorithm is specified, the SSH client will send the supported encryption algorithm list to the server for algorithm negotiation, Otherwise, the SSH client will sent only the specified encryption algorithm to the server, If the server does not support the encryption algorithm, the session will be closed.
	-l *username*	(Mandatory) The login username.
	-m { **hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160** }	(Optional) Specifies a Hash-based message authentication code (HMAC). SSHv1 does not support HMACs. If the user specifies SSHv1 and HMACs at the same time, the HMACs configuration does not take effect. If no algorithm is specified, the SSH client will send the supported

	HMAC algorithm list to the server for algorithm negotiation, Otherwise, the SSH client will sent only the specified HMAC algorithm to the server, If the server does not support the HMAC algorithm, the session will be closed.
-p *port-num*	(Optional) Specifies the port number that is used to connect to the SSH server. The port number is 22 by default.
ip-addr | *hostname*	(Mandatory) Specifies the IPv4/IPv6 address or host name for the SSH server,
/source	Specifies the source IP address or the source interface for the SSH client.
ip A.B.C.D	Specifies the source IPv4 address for the SSH client.
ipv6 X:X:X:X::X	Specifies the source IPv6 address for the SSH client.
interface *interface-name*	Specifies the source interface for the SSH client.
/vrf *vrf-name*	Specifies the VRF routing table to be queried.

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use the **ssh** command to create a secure and encrypted session between the current device (SSH client) and the other device (SSH server, or the server that supports SSHv1 or SSHv2). This session is similar to the Telnet session except that the SSH session is encrypted. Therefore, the SSH client can create a secure session on the insecure network based on authentication and encryption.

- SSHv1 supports only DES (56-bit key) and 3DES (168-bit key).
- SSHv2 supports the following AES algorithm: ase128-cbc, aes192-cbc, and aes256-cbc.
- SSHv1 does not support HMAC algorithm.
- If the specified SSH version is incompatible with the specified encryption algorithm or authentication algorithm, the algorithm configuration does not take effect.

Configuration Examples The following example creates a session with the username **admin** to the SSH server whose IP address is 192.168.23.122 via SSH.

```
Hostname#ssh -l admin 192.168.23.122
```

The following example creates a session with the username admin to the SSH server whose IP address is 192.168.23.122 via SSHv2, setting aes128-cbc and hmac-md5-128 as encryption algorithm and authentication algorithm respectively.

```
Hostname#ssh -v 2 -c aes128-cbc  -m hmac-md5-128 -l admin 192.168.23.122
```

Related Commands

Command	Description
N/A	N/A

10.25 ssh session

Use this command to restore the suspended SSH client session.

ssh-session *session-id*

Parameter Description	**Parameter**	**Description**
	session-id	ID of the SSH client session to be restored

Defaults N/A

Command Mode User EXEC mode

Usage Guide After creating the SSH client session via the **SSH** command, you can use the hot key (ctrl+shift+6 x) to temporarily suspend the session, If you want to restore the suspended SSH client session, run the **ssh-session** command. Use the **show ssh-session** command to display the established session.

Configuration Examples The following example restores the suspended SSH client session:

```
Hostname# ssh-session 1
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

11 CPU Protection Commands

11.1 clear cpu-protect-counters

Use this command to clear the CPP statistics.

clear cpu-protect counters

Parameter Description

Parameter	Description
-	-

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the CPP statistics.s

```
Hostname(config)# clear cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              6            200           0         0         600      50
Hostname#clear cpu-protect counters
Hostname(config)#show cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              6            200           0         0         0        0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.2 clear cpu-protect-counters mboard

Use this command to clear the CPP statistics on the supervisor module.

clear cpu-protect counters mboard

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the CPP statistics on the supervisor module.

```
Hostname(config)#show cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              6            200           0         0         600      50
Hostname#clear cpu-protect counters mboard
Hostname(config)#show cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              6            200           0         0         0        0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.3 cpu-protect cpu bandwidth

Use this command to configure the bandwidth for the CPU port. Use the **no** form of this command to restore the default setting.

cpu-protect cpu bandwidth *bandwidth_value*

no cpu-protect cpu bandwidth

Parameter Description

Parameter	Description
bandwidth_value	An integer number ranges from 0 to 100000 (PPS). Indicates the bandwidth value of the CPU port.

Defaults The default CPU port bandwidth varies with products.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the CPU port bandwidth to 32000pps.

```
Hostname# configure terminal
Hostname(config)# cpu-protect cpu bandwidth 32000
Hostname#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.4 cpu-protect traffic-class bandwidth

Use this command to configure the bandwidth for each priority queue. Use the **no** form of this command to restore the default setting.

cpu-protect traffic-class *traffic-class-num* **bandwidth** *bandwidth_value*

no cpu-protect traffic-class *traffic-class-num* **bandwidth**

Parameter Description

Parameter	Description
traffic-class-num	Indicates the queue priority.
bandwidth_value	An integer number ranges from 0 to 100000 (pps). Indicates the bandwidth value of the CPU port.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example s sets the priority queue 5 to 3500 pps.

```
Hostname# configure terminal
Hostname(config)# cpu-protect traffic-class 5 bandwidth 3500
Hostname#show cpu-protect traffic-class 5
Traffic-class   Bandwidth(pps)  Rate(pps)      Drop(pps)
-------------   --------------  ---------      ---------
 5            3500          0             0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.5 cpu-protect type bandwidth

Use this command to configure the bandwidth of a specific packet.

Use the **no** form of this command to restore the default setting.

cpu-protect type *packet-type* **bandwidth** *bandwidth_value*

no cpu-protect type *packet-type* **bandwidth**

Parameter Description

Parameter	Description
packet-type	Packet types classified by the switch.
bandwidth_value	An integer number ranges from 0 to 32000 (pps). Indicates the bandwidth value of the CPU port.

Defaults The default CPU port bandwidth varies with products.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the BPDU bandwidth to 200 pps.

```
Hostname# configure terminal
Hostname(config)# cpu-protect type bpdu bandwitdth 200
Hostname(config)#show cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
```

```
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              6            200             0          0          0          0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.6 cpu-protect type traffic-class

Use this command to set the priority queue (PQ) of the packet.

Use the **no** form of this command to restore the default setting.

cpu-protect type *packet-type* **traffic-class** *traffic-class-num*

no cpu-protect type *packet-type* **traffic-class**

Parameter Description	Parameter	Description
	packet-type	Packet types classified by the switch.
	traffic-class-num	Indicates the queue priority

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PQ of BPDU packets to 5.

```
Hostname# configure terminal
Hostname(config)# cpu-protect type bpdu traffic-class 5
Hostname(config)#show cpu-protect type bpdu
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total    Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu              5            200             0          0          0          0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.7 show cpu-protect

Use this command to display all CPP configuration and statistics.

show cpu-protect

Parameter Description

Parameter	Description
-	-

Defaults N/A

Command Mode All configuraiton mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.8 show cpu-protect cpu

Use this command to display the configurations of the CPU port.

show cpu-protect cpu

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example displays the configuration of the CPU port.

```
Hostname#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.9 show cpu-protect mboard

Use this command to display the statistics of various packets of CPU protection on the management board.

show cpu-protect mboard

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide This command displays the statistics of the packets received by CPU on the management board.

Configuration Examples The following example shows the output after the **show cpu-protect mboard** command is run.

```
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
tunnel-bpdu         5              128             0          0          0         0
tunnel-gvrp         5              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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.10 show cpu-protect summary

Use this command to display the CPP configuration and statistics of the master device.

show cpu-protect summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example shows the output after the **show cpu-protect summary** command is run.

```
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
tunnel-bpdu	2	128	0	0	0	0
tunnel-gvrp	2	128	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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.11 show cpu-protect traffic-class

Use this command to display the summarized configuration and statistics of priority queues.

show cpu-protect traffic-class {*traffic-class-num* **| all}**

Parameter Description

Parameter	Description
traffic-class-num	Indicates the queue priority.
all	Displays configurations and statistics of all priority queues.

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example displays the summarized configuration and statistics of priority queues.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.12 show cpu-protect type

Use this command to display the statistics of the specified type of packets

show cpu-protect type *packet-type*

Parameter Description

Parameter	Description
packt-type	Packet type, which varies with products
all	Displays the configurations and statistics of all packet types.

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example displays the statistics of the ICMP packets.

```
Hostname(config)#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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12 DHCP Snooping Commands

12.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.

clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
mac	Specifies the user MAC address to be cleared.
vlan-id	Specifies the ID of the VLAN to be cleared.
ip	Specifies the IP address to be cleared.
interface-id	Specifies the ID of the interface to be cleared.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

Configuration Examples The following example clears the dynamic database information from the DHCP Snooping binding database.

```
Hostname# clear ip dhcp snooping binding
Hostname# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- -------- ---- ---------
```

Related Commands

Command	Description
show ip dhcp snooping binding	Displays the information of the DHCP Snooping binding database.

Platform Description N/A

12.2 ip dhcp snooping

Use this command to enable the DHCP Snooping function globally.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping

no ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

Configuration Examples The following example enables the DHCP Snooping function.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of DHCP Snooping.
ip dhcp snooping vlan	Configures DHCP Snooping enabled VLAN.

Platform Description N/A

12.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

Configuration Examples The following example enables the DHCP Snooping BOOTP-bind function.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping bootp-bind
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

12.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

ip dhcp snooping check-giaddr

no ip dhcp snooping check-giaddr

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.

After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

Configuration Examples The following example enables DHCP Snooping to support the function of processing Relay requests.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping check-giaddr
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description N/A

12.5 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping database write-delay *time*

no ip dhcp snooping database write-delay

Parameter Description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

Too fast writing will reduce flash durability.

Configuration Examples The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-delay 3600
```

```
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description N/A

12.6 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to write the dynamic user information of the DHCP binding database into flash in real time.

Configuration Examples The following example writes the dynamic user information of the DHCP binding database into flash.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-to-flash
Hostname(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.7 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option [**standard-format**]

no ip dhcp snooping information option [**standard-format**]

Parameter Description

Parameter	Description
standard-format	The option82 uses the standard format.

Defaults This function is disabled by default,

Command Mode Global configuration mode

Usage Guide This command adds option82 to the DHCP request messages based on which the DHCP server assigns IP addresses.

By default, this function is in extended mode.

DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option82 and DHCP Relay at the same time.

Configuration Examples The following example adds option82 to the DHCP request message.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

12.8 ip dhcp snooping information option format remote-id

Use this command to set the option82 sub-option remote-id as the customized character string.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

no ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

Parameter

Parameter	Description

Description

string *ascii-string*	The content of the option82 remote-id extension format is customized character string.
hostname	The content of the option82 remote-id extension format hostname

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.

Configuration Examples The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option format remote-id
hostname
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.9 ip dhcp snooping information option strategy

Use this command to configure Option82 strategy.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping information option strategy {keep | drop | replace}
no ip dhcp snooping information option strategy

Parameter Description

Parameter	Description
keep	Indicates reception of request packets with Option82. Option82 is kept and the packets are forwarded.
drop	Indicates reception of request packets with Option82. The packets are dropped.
replace	Indicates reception of request packets with Option82. Option82 of the packets are replaced with Option82 configured latest. The packets are forwarded.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command only works for request packets with Option82.
If strategy is “keep” or “drop”, trailing padding is not needed for request packets with Option82.
If strategy is “replace”, trailing padding is needed for request packets with Option82.
Request packets without Option82 are padded with trailing.

Configuration Examples The following example sets “keep” as strategy.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option strategy keep
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.10 ip dhcp snooping loose-forward

Use this command to enable DHCP Snooping loose forwarding.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping loose-forward
no ip dhcp snooping loose-forward

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this feature is enabled, when the capacity of DHCP Snooping binding entries is reached, DHCP packets of new users are forwarded and obtain addresses, but DHCP Snooping does not record binding entries of new users.

Configuration Examples The following example enables DHCP Snooping loose forwarding.

```
Hostname# configure terminal
```

```
Hostname(config)# ip dhcp snooping loose-forward
Hostname(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.11 ip dhcp snooping suppression

Use this command to set the port to be the suppression status.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping suppression
no ip dhcp snooping suppression

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.
This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration Examples The following example sets **fastethernet** 0/2 to be in the suppression status.

```
Hostname# configure terminal
Hostname(config)# interface fastEthernet 0/2
Hostname(config-if)# ip dhcp snooping suppression
Hostname(config-if)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

12.12 ip dhcp snooping trust

Use this command to set the trusted ports for DHCP Snooping.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping trust
no ip dhcp snooping trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults All ports are untrusted by default.

Command Mode Interface configuration mode

Usage Guide Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration Examples The following example sets fastEthernet 0/1 as a trusted port:

```
Hostname# configure terminal
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip dhcp snooping trust
Hostname(config-if)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

12.13 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Parameter

Parameter	Description

Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

Configuration Examples The following example enables the check of the source MAC address of the DHCP request message.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping verify mac-address
Hostname(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

12.14 ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }
no ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }

Parameter Description

Parameter	Description
vlan-rng	VLAN range of effective DHCP Snooping
vlan-min	Minimum VLAN of effective DHCP Snooping
vlan-max	Maximum VLAN of effective DHCP Snooping

Defaults By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command Mode Global configuration mode

Usage Guide Use this command to enable DHCP Snooping for specified VLANs globally.

Configuration Examples The following example enables the DHCP Snooping function in VLAN 1000.

```
Hostname# configure terminal
Hostname(config)# ip dhcp snooping vlan 1000
Hostname(config)# end
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP Snooping globally.

Platform Description N/A

12.15 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

no ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

Parameter Description

Parameter	Description
vlan-word	The VLAN range
user-number	The maximum number of users bound with the VLAN

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

Configuration Examples The following example sets the maximum number of users bound with VLAN 1 to 10 and VLAN 20 to 30 respectively.

```
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
Hostname(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.16 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*
no ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter Description

Parameter	Description
vlan-id	The ID of the VLAN to be replaced

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide With this command configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

Configuration Examples The following adds the option82 to the DHCP request packets and changes the VLAN 4094 in the option82 sub-option circuit-id to VLAN93:

```
Hostname# configure terminal
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
Hostname(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.17 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*
no ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter Description

Parameter	Description
vlan-id	The VLAN where the DHCP request packets are
ascii-string	The user-defined content to fill to the Circuit ID

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized with 3 to 63 bytes, and the DHCP server will assign the addresses according the option82 information.

Configuration Examples The following example adds the option82 to the DHCP request packets with the content of the sub-option circuit-id as *port-name*.

```
Hostname# configure terminal
Hostname(config)# interface fastEthernet 0/1
Hostname(config-if)# ip dhcp snooping vlan 4094 information option format-type
circuit-id string port-name
Hostname(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.18 renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

renew ip dhcp snooping database

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to import the flash file information to the DHCP Snooping database in real time.

Records out of lease time and repeated will be neglected.

Configuration Examples The following example imports the flash file information to the DHCP Snooping database.

```
Hostname# renew ip dhcp snooping database
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.19 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

show ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
The following example displays the DHCP Snooping configuration.
Hostname# show ip dhcp snooping
```

```
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                                    Trusted           Rate
limit(pps)
------------------------                      ----------------
----------------
GigabitEthernet 0/4                            YES              unlimited
Default                                       No
```

Related Commands

Command	Description
ip dhcp snooping	Enables the DHCP Snooping globally.
ip dhcp snooping verify mac-address	Enables the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Sets the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Adds option82 to the DHCP request message.
ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.
ip dhcp snooping trust	Sets the port as a trust port.

Platform Description N/A

12.20 show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.

show ip dhcp snooping binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display all the information of the DHCP Snooping binding database.

Configuration 1: The following example displays the information of the DHCP Snooping binding database.

Examples

```
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
```

Parameter	Description
Total number of bindings	The total number of bindings in the DHCP Snooping database.
NO.	The record order.
MacAddress	The MAC address of the user.
IpAddress	The IP address of the user.
Lease(sec)	The lease time of the record.
Type	The record type.
VLAN	The VLAN where the user belongs.
Interface	The user’s connection interface. It can be a either a wired access interface or wireless access WLAN.

13 DAI Commands

13.1 ip arp inspection trust

Use this command to configure the L2 port to a trusted port.
Use the **no** form of this command to restore the L2 port to an untrusted port.
ip arp inspection trust
no ip arp inspection trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults The L2 port is untrusted.

Command Mode Interface configuration mode

Usage Guide If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Configuration Examples The following example sets the gigabitEthernet 0/19 interface as the trusted port.

```
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/19
Hostname(config-if-GigabitEthernet 0/19)# ip arp inspection trust
Hostname(config-if-GigabitEthernet 0/19)# end
```

Related Commands

Command	Description
show ip arp inspection interface	Displays related DAI information on the interface, including the trust state and rate limit of the interface.

Platform Description N/A

13.2 ip arp inspection vlan

Use this command to configure the DAI function on the VLAN.
Use the **no** form of this command to disable this function.

ip arp inspection vlan { *vlan-id* | *word* }

no ip arp inspection vlan { *vlan-id* | *word* }

Parameter Description

Parameter	Description
vlan-id	VLAN ID, ranging from 1 to 4094
word	String of the VLAN range, such as 1,3-5,7,9-11

Defaults The DAI function on all VLANs is disabled by default.

Command Mode Global configuration mode

Usage Guide To make this command take effect, you need to enable the ARP Check function first,

Not all ports of the VLAN support the ARP packet detection function. For example, the DHCP Snooping Trust port does not support any security detection, including this function.

Configuration Examples The following example detects the received ARP packets on the VLAN1 interfaces:

```
Hostname# configure terminal
Hostname(config)# ip arp inspection
Hostname(config)# ip arp inspection vlan 1
Hostname(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.3 show ip arp inspection interface

Use this command to verify whether the interface is a DAI trust interface.

show ip arp inspection interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to verify whether the interface is a DAI trust interface.

Configuration Examples The following example verifies the DAI trust state of all :

```
Hostname#show ip arp inspection interface
Interface       Trust State
--------------------   -----------
GigabitEthernet 0/1     Untrusted
Default                      Untrusted
```

Parameter Description:

Parameter	Description
Interface	Interface name.
Trust State	DAI trust state.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.4 show ip arp inspection vlan

Use this command to verify whether the DAI function on the VLAN is enabled.

show ip arp inspection vlan [*vlan-id* | *word*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID, ranging from 1 to 4094
word	String of the VLAN range, such as 1,3-5,7,9-11

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to verify whether the DAI function on the VLAN is enabled.

Configuration Examples The following example verifies whether the DAI function on the VLAN is enabled:

```
Hostname# show ip arp inspection vlan
Vlan    Configuration
----    -------------
```

```
1                                                    Active
```

Parameter Description:

Parameter	Description
Vlan	VLAN number.
Configuration	DAI status (active / inactive)

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14 IP Source Guard Commands

14.1 ip source binding

Use this command to add static user information to IP source address binding database.
Use the **no** form of this command to delete static user information from IP source address binding database.
ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| ip-mac | ip-only** }
no ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| ip-mac | ip-only** }

Parameter Description

Parameter	Description
mac-address	Adds user MAC address statically.
vlan-id	Adds user VLAN ID statically.
ip-address	Adds user IP address statically.
interface-id	Adds user interface ID statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Defaults No static address is added by default.

Command Mode Global configuration mode

Usage Guide This command allows specific clients to go through IP source guard detection instead of DHCP.
This command is supported on the wired L2 switching port, AP port and sub interface.
This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

A static IPv6 source binding is valid either on wired and WLAN interfaces or in global configuration mode.

A new binding will overwrite the old one sharing the same configuration.

Configuration Examples The following example adds the interface Id of static users.

```
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
GigabitEthernet 0/1
Hostname(config)# end
```

The following example adds static user information based on IP-MAC binding.

```
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
Hostname(config)# end
```

The following example adds static user information based on IP binding.

```
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Hostname(config)# end
```

Related Commands

Command	Description
show ip source binding	Displays the binding information of IP source address and database.

Platform Description N/A

14.2 ip verify source

Use this command to enable IP Source Guard function on the interface.

Use the **no** form of this command to restore the default setting.

ip verify source [**port-security**]

no ip verify source

Parameter Description

Parameter	Description
port-security	Configures IP Source Guard to do IP+MAC-based detection.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

This command is supported on the wired L2 switching port, AP port and sub interface.

IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Configuration Examples The following example enables IP-based IP Source Guard function.

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
Hostname(config-if)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip verify source port-security
Hostname(config-if)# end
```

Related Commands

Command	Description
show ip verify source	Displays user filtering entry of IP Source Guard.

Platform Description N/A

14.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

Use the **no** form of this command to restore the function.

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	The ID of VLAN excluded from the IP source guard configuration.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide

This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.

Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.

This command is supported on the wired L2 switching port, AP port and sub interface.

Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

Configuration Examples The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
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
Hostname(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
ip-address	Displays user binding information of corresponding IP.
mac-address	Displays user binding information of corresponding MAC.
dhcp-snooping	Displays binding information of dynamic user.
static	Displays binding information of static user.
vlan-id	Displays user binding information of corresponding VLAN.
interface-id	Displays user binding information of corresponding interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the binding information of IP source guard addresses and database.

```
Hostname# show ip source binding static
Hostname#show ip source binding static
Total number of bindings: 5
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
```

```
0/5
3       0001.0002.0003      1.2.3.4         Infinite      Static        1      Global
4       0001.0002.0004      1.2.3.5         Infinite      Static        1      Global
```

Related Commands

Command	Description
ip source binding	Sets the binding static user.

Platform Description N/A

14.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Displays user filtering entry of corresponding interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”

Now, IP Source Guard supports the following filtering modes:

inactive-restrict-off: the IP Source Guard is disabled on bound interfaces.

inactive--not-apply: the IP Source Guard cannot adds bound entries into filtering entries for system errors.

active: the IP Source Guard is active.

Configuration Examples The following example displays user filtering entry of IP Source Guard.

```
Hostname # show ip verify source
Total number of bindings: 7
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     GigabitEthernet 0/5  IP-ONLY    Active              1.2.3.4
0001.0002.0004  1 DHCP-Snooping
```

```
3    Global             IP-ONLY    Active              1.2.3.7
0001.0002.0007  1 Static
4    Global             IP+MAC     Active              1.2.3.6
0001.0002.0006  1 Static
5    GigabitEthernet 0/1  UNSET      Inactive-restrict-off  1.2.3.9
0001.0002.0009  1 DHCP-Snooping
6    GigabitEthernet 0/5  IP-ONLY    Active               Deny-All
```

Related Commands

Command	Description
ip verify source	Sets IP Source Guard on the interface.

Platform Description N/A

15 NFPP Commands

15.1 arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.
Use the **no** or **default** form of this command to restore the default setting.
arp-guard attack-threshold { **per-src-ip** | **per-src-mac** | **per-port** } *pps*
no arp-guard attack-threshold { **per-src-ip** | **per-src-mac** | **per-port** }
default arp-guard attack-threshold { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range from 1 to 19,999 in unit of pps.

Defaults By default, the global ARP guard attack threshold based on the source IP address and the source MAC address are both 200 pps. And that based on the source port is 400 pps.

Command Mode NFPP configuration mode.

Usage Guide The attack threshold shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the global ARP guard attack threshold. The attack threshold based on the source IP address is set to 2 pps. The attack threshold based on the source MAC address is set to 3 pps and that based on the source port is set to 50 pps.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Hostname(config-nfpp)# arp-guard attack-threshold per-port 50
```

Verification Run the **show nfpp arp-guard summary** command to check configuration.

Platform Description N/A

15.2 arp-guard enable

Use this command to enable the anti-ARP guard function globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard enable

no arp-guard enable

default arp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the anti-ARP guard function globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard enable
```

Related Commands

Command	Description
nfpp arp-guard enable	Enables the anti-ARP attack on the interface.
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.3 arp-guard isolate-period

Use this command to set the arp-guard isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard isolate-period { *seconds* | **permanent** }

no arp-guard isolate-period

default arp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0, or in the range from 30 to 86400 in the unit of seconds.

permanent	Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the arp-guard isolate time globally to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp arp-guard isolate-period	Sets the isolate time on the interface.
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.4 arp-guard isolate-forwarding enable

Use this command to enable packet forwarding through NFPP isolation.
Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.
arp-guard isolate-forwarding enable
no arp-guard isolate-forwarding enable
default arp-guard isolate-forwarding enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables packet forwarding through NFPP isolation.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-forwarding enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.5 arp-guard monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.
arp-guard monitored-host-limit *number*
no arp-guard monitored-host-limit
default arp-guard monitored-host-limit

Parameter Description	Parameter	Description
	number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitored-host-limit 200
```

Related Commands	Command	Description
	show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.6 arp-guard monitor-period

Use this command to configure the arp guard monitor time.
Use the **no** or **default** form of this command to restore the default setting.
arp guard monitor-period *seconds*
no arp-guard monitor-period
default arp-guard monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the arp guard monitor time to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard hosts	Displays the monitored host list.
clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description N/A

15.7 arp-guard rate-limit

Use this command to set the arp guard rate limit.
Use the **no** or **default** form of this command to restore the default setting.
arp-guard rate-limit { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

no arp-guard rate-limit { **per-src-ip | per-src-mac | per-port** }
default arp-guard rate-limit { **per-src-ip | per-src-mac | per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults By default, the global ARP guard attack threshold based on the source IP address and the source MAC address are both 30 pps. And that based on the source port is 256 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the arp guard rate limit.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# arp-guard rate-limit per-src-mac 3
Hostname(config-nfpp)# arp-guard rate-limit per-port 50
```

Related Commands

Command	Description
nfpp arp-guard policy	Sets the rate limit and the attack threshold.
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.8 arp-guard ratelimit-forwarding enable

Use this command to set the port based arp guard rate limit.
Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.
arp-guard ratelimit-forwarding enable
no arp-guard ratelimit-forwarding enable
default arp-guard ratelimit-forwarding enable

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the port based arp guard rate limit.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.9 arp-guard scan-threshold

Use this command to set the global scan threshold.
Use the **no** or **default** form of this command to restore the default setting.
arp-guard scan-threshold *pkt-cnt*
no arp-guard scan-threshold
default arp-guard scan-threshold

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999 in the unit of seconds.

Defaults The default scan threshold is 10 pps.

Command Mode NFPP configuration mode

Usage Guide The scanning may occur on the condition that:

- More than 15 packets are received within 10 seconds;
- The source MAC address for the link layer is constant while the source IP address is uncertain;
- The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

Configuration Examples The following example sets the global scan threshold to 20pps.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard scan-threshold 20
```

Related Commands

Command	Description
nfpp arp-guard scan-threshold	Sets the scan threshold on the port.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard scan	Displays the ARP guard scan table.
clear nfpp arp-guard scan	Clears the ARP guard scan table.

Platform Description N/A

15.10 clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
ip-address	Sets the IP address.
mac-address	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the monitored host isolation.

```
Hostname# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
nfpp arp-guard policy	Sets the limit threshold and attack threshold.
show nfpp arp-guard hosts	Displays the monitored host.

Platform N/A

Description

15.11 clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

clear nfpp arp-guard scan

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears ARP scanning table.

```
Hostname# clear nfpp arp-guard scan
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
nfpp arp-guard policy	Sets the attack threshold.
show nfpp arp-guard scan	Displays the ARP scanning table.

Platform Description N/A

15.12 clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to release it.

clear nfpp define *name* **hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]

Parameter Description

Parameter	Description
name	Defines guard name
vid	VLAN ID
interface-id	Interface name
ip-address	IP address
ipv6-address	IPv6 address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts in the self-defined range.

Configuration Examples The following example clears the monitored hosts.

```
Hostname# clear nfpp define tcp hosts vlan 1 interface g 0/1
```

Related Commands

Command	Description
show nfpp define hosts	Displays the isolated hosts.

Platform Description N/A

15.13 clear nfpp dhcp-guard hosts

Use this command to clear the DHCP monitored hosts, that it, release them from isolation.

clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
mac-address	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration Examples The following example clears the DHCP monitored hosts.

```
Hostname# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
dhcp-guard attack-threshold	Sets the global attack threshold.
nfpp dhcp-guard policy	Sets the limit threshold and attack threshold.

show nfpp dhcp-guard hosts	Displays the monitored host.

Platform Description N/A

15.14 clear nfpp dhcpv6-guard hosts

Use this command to clear the DHCPv6 monitored host isolation.

clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
mac-address	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts

Configuration Examples The following example clears the DHCPv6 monitored hosts.

```
Hostname# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
nfpp dhcpv6-guard policy	Sets the limit threshold and attack threshold.
show nfpp dhcpv6-guard hosts	Displays the monitored host.

Platform Description N/A

15.15 clear nfpp icmp-guard hosts

Use this command to clear the ICMP monitored hosts.

clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.

interface-id	Sets the interface name and number.
ip-address	Sets the IP address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration Examples The following example clears the ICMP monitored hosts.

```
Hostname# clear nfpp icmp-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.
nfpp icmp-guard policy	Sets the limit threshold and attack threshold.
show nfpp icmp-guard hosts	Displays the monitored host.

Platform Description N/A

15.16 clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp ip-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
ip-address	Sets the IP address.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration Examples The following example clears the monitored host isolation.

```
Hostname# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
nfpp ip-guard policy	Sets the limit threshold and attack threshold.
show nfpp ip-guard hosts	Displays the monitored host.

Platform Description N/A

15.17 clear nfpp nd-guard hosts

Use this command to remove the speed limit on the monitored host.

clear nfpp nd-guard hosts [**vlan** *vid*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command without any parameter is used to remove speed limit on all monitored hosts.

Configuration Examples The following example removes speed limit on interface g0/1 in VLAN 1.

```
Hostname# clear nfpp nd-guard hosts vlan 1 interface g0/1
```

Prompt Messages N/A

Platform Description N/A

15.18 clear nfpp log

Use this command to clear the NFPP log buffer area.

clear nfpp log

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the NFPP log buffer area.

```
Hostname# clear nfpp log
```

Related Commands

Command	Description
show nfpp log	Displays the NFPP log configuration or the log buffer area.

Platform Description N/A

15.19 cpu-protect sub-interface { manage | protocol | route } percent

Use this command to configure the percent value of each type of packets occupied in the buffer area.
Use the **no** or **default** form of this command to restore the default setting.
cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent** *percent_value*
no cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent**
default cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent**

Parameter Description

Parameter	Description
percent_value	The percent value, in the range from 1 to 100.

Defaults The default percent values of each type of packets occupied in the buffer area are:
Manage packets: 30;
Route packets: 25;
Protocol packets: 45.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the percent value of management packets in the buffer area to 60.

```
Hostname(config)# cpu-protect sub-interface manage percent 60
```

Related Commands

Command	Description
cpu-protect sub-interface { **manage** | **protocol** | **route** } *pps*	Configures the traffic bandwidth of each type of packets.

Platform Description N/A

15.20 cpu-protect sub-interface { manage | protocol | route } pps

Use this command to configure the traffic bandwidth of each type of packets.
Use the **no** or **default** form of this command to restore the default setting.
cpu-protect sub-interface { **manage** | **protocol** | **route** } **pps** *pps_vaule*
no cpu-protect sub-interface { **manage** | **protocol** | **route** } **pps**
default cpu-protect sub-interface { **manage** | **protocol** | **route** } **pps**

Parameter Description

Parameter	Description
pps_value	The rate limit threshold, in the range from 1 to 100,000

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the traffic bandwidth of management packets to 2,000 pps.

```
Hostname(config)# cpu-protect sub-interface manage pps 2000
```

Related Commands

Command	Description
cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent**	Configures the percent value of each type of packets occupied in the buffer area.

Platform Description N/A

15.21 define

Use this command to define the anti-attack type.

Use the **no** or **default** form of this command to restore the default setting.

define *name*

no define *name*

default define *name*

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide Use this command to define the anti-attack type.

Configuration Examples The following example creates the user-defined anti-attack type.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)#
```

Related Commands

Command	Description
show nfpp define summary	Displays the defined anti-attack configuration.

Platform Description N/A

15.22 define *name* enable

Use this command to enable the user-defined anti-attack globally.

Use the **no** or **default** form of this command to restore the default setting.

define *name* **enable**

no define *name* **enable**

default define *name* **enable**

Parameter Description

Parameter	Description
name	Defines guard name.

Defaults This function is disabled by default.

Command Mode NFPP configuration mode

Usage Guide This command takes effect only after the match, rate-limit and attack-threshold have been configured.

Configuration Examples The following example enabled the user-defined anti-attack globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)#define tcp enable
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

15.23 dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard attack-threshold { **per-src-mac** | **per-port** } *pps*

no dhcp-guard attack-threshold { **per-src-mac** | **per-port** }

default dhcp-guard attack-threshold { **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults By default, the global DHCP guard attack threshold based on the source MAC address is 10 pps. And that based on the source port is 512 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Hostname(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

Related Commands

Command	Description
nfpp dhcp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the monitored host.

Platform Description N/A

15.24 dhcp-guard enable

Use this command to enable the DHCP anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard enable

no dhcp-guard enable

default dhcp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the DHCP anti-attack function.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.25 dhcp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard isolate-period { *seconds* | **permanent** }

no dhcp-guard isolate-period

default dhcp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command Mode NFPP configuration mode

Usage Guide The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration Examples The following example sets the isolate time globally to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp dhcp-guard isolate-period	Sets the isolate time on the interface.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

15.26 dhcp-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard monitored-host-limit *number*

no dhcp-guard monitored-host-limit

default dhcp-guard monitored-host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

15.27 dhcp-guard monitor-period

Use this command to configure the monitor time.
Use the **no** or **default** form of this command to restore the default setting.
dhcp-guard monitor-period *seconds*
no dhcp-guard monitor-period
default dhcp-guard monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the monitor time to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the isolated host.

Platform Description N/A

15.28 dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally.
Use the **no** or **default** form of this command to restore the default setting.
dhcp-guard rate-limit { **per-src-mac | per-port** } *pps*
no dhcp-guard rate-limit { **per-src-mac | per-port** }
default dhcp-guard rate-limit { **per-src-mac | per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults By default, the global DHCP guard attack threshold based on the source MAC address is 5 pps. And that based on the source port is 300 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
Hostname(config-nfpp)# dhcp-guard rate-limit per-port 100
```

Related Commands

Command	Description
nfpp dhcp-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

15.29 dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard attack-threshold { **per-src-mac** | **per-port** } *pps*

no dhcpv6-guard attack-threshold {**per-src-mac** | **per-port**}

default dhcpv6-guard attack-threshold { **per-src-mac** | **per-port**}

Parameter Description

Parameter	Description
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range is from 1 to 19,999 pps.

Defaults By default, the global DHCPv6 guard attack threshold based on the source MAC address is 10 pps. And that based on the source port is 512 pps.

Command Mode NFPP configuration mode

Usage Guide N/A.

Configuration Examples The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

Related Commands

Command	Description

nfpp dhcpv6-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host list.
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

Platform Description N/A

15.30 dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard enable

no dhcpv6-guard enable

default dhcpv6-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the DHCPv6 anti-attack function globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.31 dhcpv6-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard monitored-host-limit *number*
no dhcpv6-guard monitored-host-limit
default dhcpv6-guard monitored-host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description N/A

15.32 dhcpv6-guard monitor-period

Use this command to configure the monitor time.
Use the **no** or **default** form of this command to restore the default setting.
dhcpv6-guard monitor-period *seconds*
no dhcpv6-guard monitor-period
default dhcpv6-guard monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of

	seconds.

Defaults The default is 600 seconds.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the monitor time to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host list.
clear nfpp dhcpv6-guard hosts	Clears the isolated host.

Platform Description N/A

15.33 dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally.
Use the **no** or **default** form of this command to restore the default setting.
dhcpv6-guard rate-limit { **per-src-mac** | **per-port** } *pps*
no dhcpv6-guard rate-limit { **per-src-mac** | **per-port** }
default dhcpv6-guard rate-limit { **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range from 1 to 19,999.

Defaults By default, the global DHCPv6 guard attack threshold based on the source MAC address is 5 pps. And that based on the source port is 300 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

Related Commands

Command	Description
nfpp dhcpv6-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description N/A

15.34 global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port.
Use the **no** or **default** form of this command to restore the default setting.
global-policy { **per-src-mac** | **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*
no global-policy { **per-src-mac** | **per-src-ip** | **per-port** }
default global-policy { **per-src-mac** | **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Performs the rate statistics based on the source IP / VID and port.
per-src-mac	Performs the rate statistics based on the source MAC / VID and port.
per-port	Performs the rate statistics based on each physical port of receiving the packets.
rate-limit-pps	Sets the rate-limit threshold.
attack-threshold-pps	Sets the attack threshold.

Defaults By default, no rate-limit threshold and attack threshold is configured. To enable self-defined anti-attack, these two parameters must be set.

Command Mode NFPP define configuration mode

Usage Guide To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is, recognize the host based on the source IP address/ source MAC address for the

user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded as an attacker. The log will be printed and the trap will be sent.

Configuration Examples The following example sets the rate-limit threshold and attack threshold based on the host or port.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nfpp define tcp
Hostname(config-nfpp-define)# global-policy per-src-ip 10  20
Hostname(config-nfpp-define)# global-policy per-port 100  200
```

Related Commands

Command	Description
nfpp define *name* **policy**	Sets the rate-limit threshold and attack threshold.
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

15.35 icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.
Use the **no** or **default** form of this command to restore the default setting.
icmp-guard attack-threshold { **per-src-ip** | **per-port** } *pps*
no icmp-guard attack-threshold { **per-src-ip** | **per-port** }
default icmp-guard attack-threshold { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range from 1 to 19,999 in the unit of pps.

Defaults By default, the global ICMP guard attack threshold based on the source IP address is 600 pps. And that based on the source port is 800 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Hostname(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

Related Commands

Command	Description
nfpp icmp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the monitored host.

Platform Description N/A

15.36 icmp-guard enable

Use this command to enable the ICMP anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard enable

no icmp-guard enable

default icmp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the ICMP anti-attack function globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard enable
```

Related Commands

Command	Description

nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.37 icmp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard isolate-period { *seconds* | **permanent** }

no icmp-guard isolate-period

default icmp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is in the range is 0 or from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command Mode NFPP configuration mode

Usage Guide The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration Examples The following example sets the isolate time globally to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp icmp-guard isolate-period	Sets the isolate time on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.38 icmp-guard monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.
icmp-guard monitored-host-limit *number*
no icmp-guard monitored-host-limit
default icmp-guard monitored-host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.39 icmp-guard monitor-period

Use this command to configure the monitor time.
Use the **no** or **default** form of this command to restore the default setting.
icmp-guard monitor-period *seconds*
no icmp-guard monitor-period

default icmp-guard monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from180 to 86,400 seconds.

Defaults The default is 600.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the monitor time to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the isolated host.

Platform Description N/A

15.40 icmp-guard rate-limit

Use this command to set the rate-limit threshold globally.
Use the **no** or **default** form of this command to restore the default setting.
icmp-guard rate-limit { **per-src-ip** | **per-port** } *pps*
no icmp-guard rate-limit { **per-src-ip | per-port** }
default icmp-guard rate-limit { **per-src-ip | per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.

pps	Sets the rate limit, in the range from1 to19,999.

Defaults By default, the global ICMP guard attack threshold based on the source IP address is 400 pps. And that based on the source port is 500 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Hostname(config-nfpp)# icmp-guard rate-limit per-port 800
```

Related Commands

Command	Description
nfpp icmp-guard policy	Sets the rate limit and the attack threshold.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.41 icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring.
Use the **no** or **default** form of this command to restore the default setting.
icmp-guard trusted-host *ip mask*
no icmp-guard trusted-host { **all** | *ip mask* }
default icmp-guard trusted-host

Parameter Description

Parameter	Description
ip	Sets the IP address.
mask	Sets the IP mask.
all	Deletes the configuration of all trusted hosts.

Defaults No trusted host is configured by default.

Command Mode NFPP configuration mode

Usage Guide The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration.

Configure the mask to set all hosts in one network segment free from monitoring.
UP to 500 trusted hosts are supported.

Configuration Examples The following example sets the trusted hosts free form monitoring.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands

Command	Description
show nfpp icmp-guard trusted-host	Displays the configuration.

Platform Description N/A

15.42 ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.
Use the **no** or **default** form of this command to restore the default setting.
ip-guard attack-threshold { **per-src-ip** | **per-port** } *pps*
no ip-guard attack-threshold { **per-src-ip** | **per-port** }
default ip-guard attack-threshold { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults By default, the global IP guard attack threshold based on the source IP address is 200 pps. And that based on the source port is 400 pps.

Command Mode NFPP configuration mode

Usage Guide The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration Examples The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# ip-guard attack-threshold per-port 50
```

Related

Command	Description

Commands

nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host list.
clear nfpp ip-guard hosts	Clears the monitored host.

Platform Description N/A

15.43 ip-guard enable

Use this command to enable IP guard.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard enable

no ip-guard enable

default ip-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode.

Usage Guide This configuration aims at attacks whose destination IP address is not the local one. For those with the local address as the destination, CPP (CPU Protect Policy) will limit their rates.

Configuration Examples The following example enables the IP guard globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard enable
```

Related Commands

Command	Description
nffp ip-guard enable	Enables the IP guard on the interface.

Platform Description N/A

15.44 ip-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard isolate-period { *seconds* | **permanent** }

no ip-guard isolate-period

default ip-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0 or in the range from 30 to 86, 400 in the unit of seconds.
permanent	Permanent isolation

Defaults The default isolate time is 0 second, which means no isolation.

Command Mode NFPP configuration mode

Usage Guide N/A.

Configuration Examples The following example sets the isolate time globally to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard isolate-period 180
```

Related Commands

Command	Description
nfpp ip-guard isolate-period	Sets the isolate time on the interface.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.45 ip-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard monitor-period *seconds*

no ip-guard monitor-period

default ip-guard monitor-period

Parameter Description

Parameter	Description

seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software

Configuration Examples The following example sets the monitor time to 180 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host list.
clear nfpp ip-guard hosts	Clears the isolated host.

Platform Description N/A

15.46 ip-guard monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.
ip-guard monitored-host-limit *number*
no ip-guard monitored-host-limit
default ip-guard monitored-host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000 seconds.

Command NFPP configuration mode

Mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.47 ip-guard rate-limit

Use this command to set the rate-limit threshold globally.
Use the **no** or **default** form of this command to restore the default setting.
ip-guard rate-limit { **per-src-ip** | **per-port** } *pps*
no ip-guard rate-limit { **per-src-ip | per-port** }
default ip-guard rate-limit {**per-src-ip | per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults By default, the global IP guard attack threshold based on the source IP address is 20 pps. And that based on the source port is 100 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# ip-guard rate-limit per-port 50
```

Related Commands

Command	Description
nfpp ip-guard policy	Sets the rate limit and the attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.48 ip-guard scan-threshold

Use this command to set the global scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard scan-threshold *pkt-cnt*

no ip-guard scan-threshold

default ip-guard scan-threshold

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999.

Defaults The default scan threshold of IP guard is 10 pps.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the global scan threshold to 20 pps.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard scan-threshold 20
```

Related Commands

Command	Description
nfpp ip-guard scan-threshold	Sets the scan threshold on the port.
show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

15.49 ip-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard trusted-host *ip mask*

no ip-guard trusted-host { **all** | *ip mask* }

default ip-guard trusted-host

Parameter Description

Parameter	Description
ip	Sets the IP address.
mask	Sets the IP mask.
all	Deletes the configuration of all trusted hosts.

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration.

Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Configuration Examples The following example sets the trusted hosts free form monitoring.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands

Command	Description
show nfpp ip-guard trusted-host	Displays the configuration.

Platform Description N/A

15.50 log-buffer enable

Use this command to display logs on the screen.

Use the **no** or the **default** form of this command to restore the default setting.

log-buffer enable

no log-buffer enable

default log-buffer enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Logs are stored in the cache by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example displays logs on the screen.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.51 log-buffer entries

Use this command to set the NFPP log buffer area size.

Use the **no** or **default** form of this command to restore the default setting.

log-buffer entries *number*

no log-buffer entries

default log-buffer entries

Parameter Description

Parameter	Description
number	The buffer area size, in the range from 0 to 1,024.

Defaults The default is 256.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the NFPP log buffer area size.

Examples

```
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer entries 50
```

Related Commands

Command	Description
log-buffer logs *number_of_message* **interval** *length_in_seconds*	Displays the rate of the syslog generated from the NFPP buffer area.
show nfpp log	Displays the NFPP log configuration or the log buffer area.

Platform Description N/A

15.52 log-buffer logs

Use this command to set the rate of syslog generated from the NFPP log buffer area.
Use the **no** or **default** form of this command to restore the default setting.
log-buffer logs *number_of_message* **interval** *length_in_seconds*
no log-buffer logs
default log-buffer logs

Parameter Description

Parameter	Description
number_of_message	The valid range is from 0 to1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
length_in_seconds	The valid range is from 0 to 86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter *number_of_message /length_in_second* indicates the rate of syslog generated from the NFPP log buffer area.

Defaults By default, *number_of_message* is 0 and *length_in_seconds* is 0.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate of syslog generated from the NFPP log buffer area.

```
Hostname(config)# nfpp
```

```
Hostname(config-nfpp)# log-buffer logs 2 interval 12
```

Related Commands

Command	Description
log-buffer entries *number*	Sets the NFPP log buffer area size.
show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform Description N/A

15.53 logging

Use this command to set the VLAN or the interface log for NFPP.
Use the **no** or **default** form of this command to restore the default setting.
logging vlan *vlan-range*
logging interface *interface-id*
no logging vlan *vlan-range*
no logging interface *interface-id*
default logging

Parameter Description

Parameter	Description
vlan-range	Sets the specified VLAN range, in the format such as “1-3, 5”.
interface-id	Sets the interface ID.

Defaults All logs are recorded by default.

Command Mode NFPP configuration mode

Usage Guide Use this command to filter the logs and records the logs within the specified VLAN range or the specified port

Configuration Examples The following example records the logs in VLAN 1, VLAN 2,VLAN 3 and VLAN 5 only.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# logging vlan 1-3,5
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# logging interface G 0/1
```

Related Commands

Command	Description

show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform Description N/A

15.54 match

Use this command to specify the message matching filed for the user-defined anti-attack.
match [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip* [**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]] [**src-port** *sport*] [**dst-port** *dport*]

Parameter Description

Parameter	Description
type	Ethernet link layer packet type
smac	Source MAC address
smac_mask	Source MAC address mask
dmac	Destination MAC address
dmac_mask	Destination MAC address mask
protocol	IPv4/v6 message protocol
sip	Source IPv4 address
sip_mask	Source IPv4 address mask
sipv6	Source IPv6 address
sipv6_masklen	Source IPv6 address mask
dip	Destination IPv4 address
dip_mask	Destination IPv4 address mask
dipv6	Destination IPv6 address
dipv6_masklen	Length of the destination IPv6 address mask.
sport	Source port
dport	Destination port

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide Use this command to create a new user-defined anti-attack type and specify the message fields to be matched.

Configuration Examples The following example specifies the message matching filed for the user-defined anti-attack.

```
Hostname(config)# nfpp
```

```
Hostname(config-nfpp)# nfpp define tcp
Hostname(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

15.55 monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.
monitored-host-limit *number*
no monitored-host-limit
default monitored-host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP define configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % % NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20,000 monitored hosts. to remind the administrator

Configuration Examples The following example sets the maximum monitored host number.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nfpp define tcp
Hostname(config-nfpp-define)#monitored-host-limit 500
```

Related Commands

Command	Description

show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

15.56 monitor period

Use this command to set the monitoring time.
Use the **no** or **default** form of this command to restore the default setting.
monitor-period *seconds*
no monitor-period
default monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command Mode NFPP define configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the monitoring time to 1,000 seconds.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)#monitor-period 1000
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description N/A

15.57 nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** } *pps*

no nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** }

default nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
pps	Sets the attack threshold, in the range from1 to 19999 in the unit of seconds.

Defaults By default, the ns-na global ND guard threshold based on the source port is 200 pps. The rs global ND guard threshold based on the source port is 100 pps. The ra-redirect global ND guard threshold based on the source port is 100 pps.

Command Mode NFPP configuration mode.

Usage Guide The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration Examples The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Hostname(config-nfpp)# nd-guard attack-threshold per-port rs 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

Related Commands

Command	Description
nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.58 nd-guard enable

Use this command to enable the ND anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard enable

no nd-guard enable

default nd-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the ND anti-attack function.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard enable
```

Related Commands

Command	Description
nffp nd-guard enable	Enables the ND anti-attack function on the interface.
show nfpp nd-guard summary	Displays the configuration.

Platform Description N/A

15.59 nd-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** } *pps*

no nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** }

default nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.

rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
pps	Sets the attack threshold, in the range is from 1 to 19,999 in the unit of pps.

Defaults By default, the ns-na global ND guard threshold based on the source port is 100 pps. The rs global ND guard threshold based on the source port is 50 pps. The ra-redirect global ND guard threshold based on the source port is 50 pps.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Hostname(config-nfpp)# nd-guard rate-limit per-port rs 5
Hostname(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

Related Commands

Command	Description
nfpp nd-guard policy	Sets the rate limit and the attack threshold.
show nfpp nd-guard summary	Displays the configuration.

Platform Description N/A

15.60 nd-guard ratelimit-forwarding enable

Use this command to enable the ND-guard ratelimit-forwarding on the interface.
nd-guard ratelimit-forwarding enable

Use this command to disable the ND-guard ratelimit-forwarding on the interface.
no nd-guard ratelimit-forwarding enable

Use this command to restore the default setting.
default nd-guard ratelimit-forwarding enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the ND-guard ratelimit-forwarding on the interface.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Platform Description N/A

15.61 nfpp

Use this command to enter NFPP configuration mode.

nfpp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to enter NFPP configuration mode and make further configuration.

Configuration Examples

```
Hostname(config)# nfpp
```

Platform Description N/A

15.62 nfpp arp-guard enable

Use this command to enable the anti-ARP attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard enable

no nfpp arp-guard enable

default nfpp arp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The anti-ARP attack function is not enabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface anti-ARP attack configuration is prior to the global configuration.

Configuration Examples The following example enables the anti-ARP attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp arp-guard enable
```

Related Commands

Command	Description
arp-guard enable	Enables the anti-ARP attack function.
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.63 nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard isolate-period { *seconds* | **permanent** }

no nfpp arp-guard isolate-period

default nfpp arp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period. The value is 0, or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the isolate period in the interface configuration mode.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp arp-guard isolate-period 180
```

Related Commands

Command	Description
arp-guard isolate-period	Sets the global isolate period.
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

15.64 nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** }

default nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to 19999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp arp-guard policy per-src-ip 2 10
Hostname(config-if)# nfpp arp-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp arp-guard policy per-port 50 100
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
arp-guard rate-limit	Sets the global rate-limit threshold.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard hosts	Displays the monitored host.
clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description N/A

15.65 nfpp arp-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard scan-threshold *pkt-cnt*

no nfpp arp-guard scan-threshold

default nfpp arp-guard scan-threshold

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from1 to 19,999.

Defaults By default, the sport-based scan threshold is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the scan threshold to 20 pps.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp arp-guard scan-threshold 20
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard scan	Displays the ARP scan table.
clear nfpp arp-guard scan	Clears the ARP scan table.

Platform Description N/A

15.66 nfpp define *name* enable

Use this command to enable the user-defined anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp define *name* **enable**

no nfpp define *name* **enable**

default nfpp define *name* **enable**

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.

Configuration Examples The following example enables the user-defined anti-attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp define tcp enable
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description N/A

15.67 nfpp define policy

Use this command to set the local rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp define *name* **policy** { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp define *name* **policy** {**per-src-ip | per-src-mac** | **per-port**}

default nfpp define *name* **policy** { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.

per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range of from1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the local rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp define tcp policy per-src-ip 2 10
Hostname(config-if)# nfpp define tcp policy per-port 50 100
```

Related Commands

Command	Description
define-policy	Sets the global rate-limit threshold and attack threshold.
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description N/A

15.68 nfpp dhcp-guard enable

Use this command to enable the DHCP anti-attack function on the interface.
Use the **no** or **default** form of this command to restore the default setting.
nfpp dhcp-guard enable
no nfpp dhcp-guard enable
default nfpp dhcp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The DHCP anti-attack function is not enabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface DHCP anti- attack configuration is prior to the global configuratio

Configuration Examples The following example enables the DHCP anti-attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp dhcp-guard enable
```

Related Commands

Command	Description
dhcp-guard enable	Enables the anti-ARP attack function.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

15.69 nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold on the port.
Use the **no** or **default** form of this command to restore the default setting.
nfpp dhcp-guard policy { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*
no nfpp dhcp-guard policy { **per-src-mac** | **per-port** }
default nfpp dhcp-guard policy { **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate-limit threshold and the attack threshold for the designated source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for the designated port.
rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to 19,999.

Defaults The rate-limit threshold and the attack threshold are not configured by default. So the device adopts the rate-limit threshold and the attack threshold that are set in the global configuration mode.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold on interface G0/1.

```
Hostname(config)#interface G 0/1
Hostname(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.70 nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcpv6-guard enable

no nfpp dhcpv6-guard enable

default nfpp dhcpv6-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The DHCPv6 anti-attack function is not enabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface DHCPv6 anti- attack configuration is prior to the global configuration.

Configuration Examples The following example enables the DHCPv6 anti-attack function on interface G0/1.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp dhcpv6-guard enable
```

Related Commands

Command	Description
dhcpv6-guard enable	Enables the anti-ARP attack function.
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description N/A

15.71 nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcpv6-guard policy { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp dhcpv6-guard policy { **per-src-mac** | **per-port**}

default nfpp dhcpv6-guard policy { **per-src-mac** | **per-port**}

Parameter Description

Parameter	Description
per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range of from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host.
clear nfpp dhcpv6-guard hosts	Clears the isolated host.

Platform Description N/A

15.72 nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp icmp-guard enable

no nfpp icmp-guard enable

default nfpp icmp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The ICMP anti-attack function is not enabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface ICMP anti- attack configuration is prior to the global configuration.

Configuration Examples The following example enables the ICMP anti-attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp icmp-guard enable
```

Related Commands

Command	Description
icmp-guard enable	Enables the anti-ARP attack function.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.73 nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.
Use the **no** or **default** form of this command to restore the default setting.
nfpp icmp-guard isolate-period { *seconds* | **permanent** }
no nfpp icmp-guard isolate-period
default nfpp icmp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the isolate period in the interface configuration mode.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp icmp-guard isolate-period 180
```

Related Commands

Command	Description
icmp-guard isolate-period	Sets the global isolate period.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

15.74 nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp icmp-guard policy { p**er-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp icmp-guard policy { **per-src-ip** | **per-port** }

default nfpp icmp-guard policy { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in range from1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Hostname(config-if)# nfpp icmp-guard policy per-port 100 200
```

Related Commands

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.

icmp-guard rate-limit	Sets the global rate-limit threshold.
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host.
clear nfpp icmp-guard hosts	Clears the isolated host.

Platform Description N/A

15.75 nfpp ip-guard enable

Use this command to enable the IP anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard enable

no nfpp ip-guard enable

default nfpp ip-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IP anti-attack function is disabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface IP anti-attack configuration is prior to the global configuration.

Configuration Examples The following example enables the IP anti-attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp ip-guard enable
```

Related Commands

Command	Description
ip-guard enable	Enables the anti-ARP attack function.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.76 nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard isolate-period { *seconds* | **permanent** }
no nfpp ip-guard isolate-period
default nfpp ip-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period, in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the isolate period in the interface configuration mode.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp ip-guard isolate-period 180
```

Related Commands

Command	Description
ip-guard isolate-period	Sets the global isolate period.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.77 nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold.
Use the **no** or **default** form of this command to restore the default setting.
nfpp ip-guard policy { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*
no nfpp ip-guard policy { **per-src-ip** | **per-port** }
default nfpp ip-guard policy { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.

attack-threshold-pps	Sets the attack threshold, in the range from 1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp ip-guard policy per-src-ip 2 10
Hostname(config-if)# nfpp ip-guard policy per-port 50 100
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
ip-guard rate-limit	Sets the global rate-limit threshold.
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host.
clear nfpp ip-guard hosts	Clears the isolated host.

Platform Description N/A

15.78 nfpp ip-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard scan-threshold *pkt-cnt*

no nfpp ip-guard scan-threshold

default nfpp ip-guard scan-threshold

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999.

Defaults By default, the sport-based scan threshold is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the scan threshold to 20pps.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp ip-guard scan-threshold 20
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

15.79 nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp nd-guard enable

no nfpp nd-guard enable

default nfpp nd-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The ND anti-attack function is disabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface ND anti-attack configuration is prior to the global configuration.

Configuration Examples The following example enables the ND anti-attack function on the interface.

```
Hostname(config)# interface G0/1
Hostname(config-if)# nfpp nd-guard enable
```

Related Commands

Command	Description
nd-guard enable	Enables the ND anti-attack function.
show nfpp nd-guard summary	Displays the configuration.

Platform Description N/A

15.80 nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** } *rate-limit-pps attack-threshold-pps*

no nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** }

default nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from 1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```
Hostname(config)# interface G 0/1
Hostname(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Hostname(config-if)# nfpp nd-guard policy per-port rs 10 20
Hostname(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

Related Commands

Command	Description
nd-guard attack-threshold	Sets the global attack threshold.
nd-guard rate-limit	Sets the global rate-limit threshold.
show nfpp nd-guard summary	Displays the configuration.

Platform Description N/A

15.81 show nfpp arp-guard hosts

Use this command to display the monitored host.

show nfpp arp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address* |

mac-address]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address
mac-address	The MAC address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the statistical information of the monitored host.

```
Hostname# show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host.

```
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
```

Related Commands

Command	Description
clear nfpp arp-guard hosts	Clears the monitored hosts.

Platform Description N/A

15.82 show nfpp arp-guard scan

Use this command to display the ARP scan list.

show nfpp arp-guard scan [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

[*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the ARP scan list.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address
mac-address	The MAC address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the ARP scan list.

```
Hostname# show nfpp arp-guard scan statistics
arp-guard table has 4 record(s).
```

The following example displays the ARP scan list.

```
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)
```

The following example displays the ARP scan list.

```
Hostname# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
VLAN    interface   IP address   MAC address    timestamp
----    --------    ----------    -----------    -------
1       Gi0/1      -           0000.0000.0001   2008-01-23 16:23:10
Total:1 record(s)
```

Related Commands

Command	Description
arp-guard scan-threshold	Sets the global scan threshold.
nfpp arp-guard scan-threshold	Sets the scan threshold.
clear nfpp arp-guard scan	Clears the ARP scan list.

Platform Description N/A

15.83 show nfpp arp-guard summary

Use this command to display the configuration.

show nfpp arp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
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
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
Scan-threshold	Scan threshold

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
arp-guard enable	Enables the anti-ARP attack function.
arp-guard isolate-period	Sets the global isolate time.
arp-guard monitor-period	Sets the monitor period.

arp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
arp-guard rate-limit	Sets the global rate-limit threshold.
arp-guard scan-threshold	Sets the global scan threshold.
nfpp arp-guard enable	Enables the anti-ARP attack function on the interface.
nfpp arp-guard isolate-period	Sets the isolate time.
nfpp arp-guard policy	Sets the rate-limit threshold and attack threshold.
nfpp arp-guard scan-threshold	Sets the scan threshold.

Platform Description N/A

15.84 show nfpp define hosts

Use this command to display the monitored hosts.

show nfpp define hosts *name* [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]]]

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type
statistics	Displays the statistics of monitored hosts.
vid	VLAN ID
interface-id	Interface name
ip-address	IP address
mac-address	MAC address
ipv6-address	IPv6 address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command allows filtering the hosts with parameters specified

Configuration Examples The following example displays the monitored hosts.

```
Hostname#show nfpp define hosts abc
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
```

Related Commands

Command	Description
clear nfpp define hosts	Clears the monitored hosts of user-defined anti-attack type.

Platform Description N/A

15.85 show nfpp define summary

Use this command to display the configuration.

show nfpp define summary [*name*]

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the configuration. Without the name specified, all user-defined anti-attack types will be displayed.

Configuration Examples The following example displays the configuration.

```
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  -/-/-          -/-/-
```

Field	Description
Interface	If the interface field is displayed as Global, it means that is configured in the global configuration mode.
Status	Enables/ Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/

	the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
match	Clears the monitored hosts of user-defined anti-attack type.
policy	Attack threshold and rate-limit threshold.
isolate-period	Isolates time
monitored-period	Monitored time
monitored-host-limit	Maximum monitored host number

Platform Description N/A

15.86 show nfpp define trusted-host

Use this command to display the trusted host free from monitoring.

show nfpp define trusted-host *name*

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the trusted host configuration.

```
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)
```

Related Commands

Command	Description
trusted-host	Configures the trusted hosts.

Platform Description N/A

15.87 show nfpp dhcp-guard hosts

Use this command to display the monitored host.

show nfpp dhcp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	VLAN ID
interface-id	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the monitored host.

```
Hostname# show nfpp dhcp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example displays the monitored host.

```
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)
```

Related Commands

Command	Description
clear nfpp dhcp-guard hosts	Clears the monitored host.

Platform Description N/A

15.88 show nfpp dhcp-guard summary

Use this command to display the configuration.

show nfpp dhcp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
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
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Isolate-period	Isolate period
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
dhcp-guard attack-threshold	Sets the global attack threshold.
dhcp-guard enable	Enables the DHCP anti-attack function.
dhcp-guard isolate-period	Sets the global isolate time.
dhcp-guard monitor-period	Sets the monitor period.

dhcp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
dhcp-guard rate-limit	Sets the global rate-limit threshold.
nfpp dhcp-guard enable	Enables the DHCP anti-attack function on the interface.
nfpp dhcp-guard isolate-period	Sets the isolate time.
nfpp dhcp-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description N/A

15.89 show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

show nfpp dhcpv6-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
mac-address	The MAC address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the monitored host.

```
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)
```

Related Commands

Command	Description
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

Platform Description N/A

15.90 show nfpp dhcpv6-guard summary

Use this command to display the configuration.

show nfpp dhcpv6-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
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
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
dhcpv6-guard enable	Enables the DHCPv6 anti-attack function.
dhcpv6-guard monitor-period	Sets the monitor period.

dhcpv6-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
nfpp dhcpv6-guard enable	Enables the DHCPv6 anti-attack function on the interface.
nfpp dhcpv6-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description N/A

15.91 show nfpp icmp-guard hosts

Use this command to display the monitored host.

show nfpp icmp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the monitored host.

```
Hostname# show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example displays the monitored host.

```
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)
```

Related Commands

Command	Description
clear nfpp icmp-guard hosts	Clears the monitored host.

Platform Description N/A

15.92 show nfpp icmp-guard summary

Use this command to display the configuration.

show nfpp icmp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
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
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Isolate-period	Isolate period

Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.
icmp-guard enable	Enables the ICMP anti-attack function.
icmp-guard isolate-period	Sets the global isolate time.
icmp-guard monitor-period	Sets the monitor period.
icmp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
icmp-guard rate-limit	Sets the global rate-limit threshold.
nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
nfpp icmp-guard isolate-period	Sets the isolate time.
nfpp icmp-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description N/A

15.93 show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

show nfpp icmp-guard trusted-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the trusted host free from being monitored.

```
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)
```

Related Commands

Command	Description
icmp-guard trusted-host	Sets the trusted host.

Platform Description N/A

15.94 show nfpp ip-guard hosts

Use this command to display the monitored host.

show nfpp ip-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
mac-address	The MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the monitored host.

```
Hostname# show nfpp ip-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example displays the monitored host.

```
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)
```

Related Commands

Command	Description
clear nfpp ip-guard hosts	Clears the monitored host.

Platform Description N/A

15.95 show nfpp ip-guard summary

Use this command to display the configuration.

show nfpp ip-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
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
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Isolate-period	Isolate period
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Scan-threshold	Scan threshold

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
ip-guard enable	Enables the IP anti-attack function.
ip-guard isolate-period	Sets the global isolate time.
ip-guard monitor-period	Sets the monitor period.
ip-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
ip-guard rate-limit	Sets the global rate-limit threshold.
nfpp ip-guard enable	Enables the IP anti-attack function on the interface.
nfpp ip-guard isolate-period	Sets the isolate time.
nfpp ip-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description N/A

15.96 show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

show nfpp ip-guard trusted-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the trusted host free from being monitored.

```
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)
```

Related Commands	Command	Description
	ip-guard trusted-host	Sets the trusted host.

Platform Description N/A

15.97 show nfpp log

Use this command to display the NFPP log configuration.

show nfpp log summary

Use this command to display the NFPP log buffer area content.

show nfpp log buffer [**statistics**]

Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the NFPP log buffer area.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes ”-” is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog.

The generated syslog in the log buffer area carries with the timestamp, for example:

%NFPP_ARP_GUARD-4-DOS_DETECTED:

Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

Configuration Examples The following example displays the NFPP log configuration.

```
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
```

The following example displays the log number in the buffer area.

```
Hostname#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example shows the NFPP log buffer area:

```
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
```

Field	Description
Protocol	ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT
Reason	DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED

Related Commands

Command	Description
clear nfpp log	Clears the NFPP log buffer area.

Platform Description N/A

15.98 show nfpp nd-guard summary

Use this command to display the configuration.

show nfpp nd-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
Hostname# show nfpp nd-guard summary
(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold
Global     Enable  20/5/10    40/10/20
Gi 0/1      Enable  15/15/15   30/30/30
Gi 0/2      Disable -/5/30      -/10/50
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
nd-guard attack-threshold	Sets the global attack threshold.
nd-guard enable	Enables the ND anti-attack function.
nd-guard rate-limit	Sets the global rate-limit threshold.
nfpp nd-guard enable	Enables the ND anti-attack function on the interface.
nfpp nd-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description N/A

15.99 show nfpp nd-guard hosts

Use this command to display the monitored host.

show nfpp nd-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistics of the monitored host.
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the statistics of the host monitored by ND-guard.

```
Hostname#show nfpp nd-guard hosts statistics
success    fail    total
-------    ----    -----
10         2       12
```

The following example displays the host monitored by ND-guard. The “remain-time(s)” refers to the remaining time of isolation.

```
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
```

Platform Description N/A

15.100 trusted-host

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting,

trusted-host { *mac mac_mask* | *ip mask* | *IPv6/prefixlen* }

no trusted-host {**all |** *mac mac_mask* **|** *ip mask* | *IPv6/prefixlen* }

default trusted-host

Parameter Description

Parameter	Description
ip	Sets the IP address
mac	MAC address
mac_mask	MAC address mask
IPv6/prefixlen	IPv6 address and mask length
mask	IP mask
all	Deletes the configuration of all trusted hosts with the no form of this command.

Defaults N/A

Command Mode NFPP define configuration mode

Usage Guide The administrator can use this command to set the trusted host free from monitoring. The ICMP

packets are allowed to be sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.
UP to 500 trusted hosts are supported.
Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.

Configuration Examples The following example sets the trusted hosts free form monitoring.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255
```

Related Commands

Command	Description
show nfpp define trusted-host	Displays the trusted host configuration.

Platform Description N/A

15.101 no all-guard enable

Use this command to disable all NFPP guards (except guards self-defined and enabled in interface configuration mode).
no all-guard enable
Use this command to enable all NFPP guards.
all-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode NFPP configuration mode

Usage Guide

- By default, all basic NFPP guards are enabled.
- This global command supports basic NFPP guards including ARP-GUARD, IP-GUARD, ICMP-GUARD, DHCP-GUARD, DHCPv6-GUARD and ND-GUARD.
- The **no** form command will disable all guards, which is displayed guard-by-guard by using the **show running-config** command. The exception is guards self-defined and configured in interface configuration mode.

Configuration Examples

```
Hostname(config)#show running-config  | begin nfpp
nfpp
 log-buffer enable
```

```
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
!
Hostname(config)# nfpp
Hostname(config-nfpp)#no all-guard enable
Hostname(config-nfpp)#show running-config  | begin nfpp
nfpp
 log-buffer enable
 no arp-guard enable
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
 no icmp-guard enable
 no ip-guard enable
 no dhcp-guard enable
 no dhcpv6-guard enable
 no nd-guard enable
!
Hostname(config-nfpp)#all-guard enable
Hostname(config-nfpp)#show running-config  | begin nfpp
nfpp
 log-buffer enable
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
!
no service password-encryption
!
```

Platform Description N/A

ACL & QoS Configuration Commands

1. ACL Commands
2. QoS Commands

1 ACL Commands

1.1 access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

1. Standard IP access list (1 to 99, 1300 to 1999)

access-list *id* { **deny** | **permit** } { *source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

2. Extended IP access list (100 to 199, 2000 to 2699)

access-list *id* { **deny** | **permit** } *protocol* { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

3. Extended MAC access list (700 to 799)

access-list *id* {**deny** | **permit**} {**any** | **host** *source-mac-address* | *source-mac-address mask* } {**any** | **host** *destination-mac-address* | *destination-mac-address mask* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*]

4. Extended expert access list (2700 to 2899)

access-list *id* { **deny** | **permit** } [*protocol* | [*ethernet-type*] **[cos** [*out*] **[inner** *in*]] **[VID** [*out*] **[inner** *in*]] { *source source-wildcard* **| host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** }] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

access-list *id* {**deny** | **permit**} {*ethernet-type*| **cos** [*out*][**inner** *in*]} [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

access-list *id* { **deny** | **permit** } *protocol* [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

access-list *id* { **deny** | **permit** } **icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

access-list *id* { **deny** | **permit** } **tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **host** *source-mac-address* | **any** } [**operator** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**operator** [**port**]] [{ **precedence**

precedence | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

access-list *id* { **deny** | **permit** } **udp**[**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } [**operator** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**operator** [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Parameter	Description
id	Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
deny	If not matched, access is denied.
permit	If matched, access is permitted.
source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
fragment	Packet fragment filtering
precedence	Specify the packet priority.
precedence	Packet precedence value (0 to 7)
dscp	Differentiated Services Code Point
dscp	The value of the code point in the range from 0 to 63.
range	Layer4 port number range of the packet.
lower	Lower limit of the layer4 port number.
upper	Upper limit of the layer4 port number.
time-range	Time range of packet filtering
time-range-name	Time range name of packet filtering
tos	Specify type of service.
tos	ToS value (0 to 15)
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port	Port number; range needs two port numbers, while other operators only need one port number.

host source-mac-address	Source physical address
host destination-mac-address	Destination physical address
VID vid	Match the specified VID.
ethernet-type	Ethernet type
match-all	Match all the bits of the TCP flag.
tcp-flag	Match the TCP flag.
established	Match the RST or ACK bits, not other bits of the TCP flag.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:
The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.
The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.
The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.
The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.
For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence*/**tos** *tos*/**fragments**/**range** *lower upper*/**time-range** *time-range-name*
The TCP Flag includes part or all of the following:

- urg
- ack
- psh
- rst
- syn
- fin

The packet precedence is as below:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- 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
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed

- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- 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 Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

Configuration Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
Hostname (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
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
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
Hostname(config)#access-list 702 deny host 00d0f8000c0c any aarp
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Hostname(config)#access-list 2702 deny tcp host 192.168.12.3 mac
00d0.f800.0044 any any
Hostname(config)# access-list 2702 permit any any any any
Hostname(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

Related Commands

Command	Description
show access-lists	Show all the ACLs.
mac access-group	Apply the extended MAC ACL on the interface.

Platform Description N/A

1.2 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

access-list *id* **list-remark** *text*

no access-list *id* **list-remark**

Parameter Description

Parameter	Description
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999.

	Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list.

Defaults The access lists have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

Configuration Examples The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL100.

```
Hostname(config)# ip access-list extended 100
Hostname(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

Related Commands

Command	Description
show access- lists	Displays all access lists, including the remarks for the access lists.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list.

Platform Description

1.3 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

access-list *id* **remark** *text*

no access-list *id* **remark** *text*

Parameter Description

Parameter	Description
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799.

	Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list entry.

Defaults The access list entries have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

Configuration Examples The following example writes a comment for an entry in ACL102.

```
Hostname(config)# access-list 102 remark deny-host-10.1.1.1
```

Related Commands

Command	Description
show access-lists	Displays all access lists, including the remarks for the access list entries.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list entry.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list entry.

Platform Description

1.4 clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

clear access-list counters [*id* | *name*]

Parameter Description

Parameter	Description
id	Access list number
name	Access list name

Defaults

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the counters of packets matching the deny entries in ACLs.

Configuration Examples The following example clears the packet matching counter of ACL No. 1:

Before configuration:

```
Hostname #show access-lists
ip access-list standard 1
   10 deny host 50.1.1.2 (10 matches)
   20 permit host 60.1.1.2 (15 matches)
   (10 packets filtered)
```

After configuration:

```
Hostname# end
Hostname# clear access-list counters
Hostname# show access-lists
ip access-list standard 1
   10 deny host 50.1.1.2 (10 matches)
   20 permit host 60.1.1.2 (15 matches)
```

Related Commands

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Platform Description N/A

1.5 clear counters access-list

Use this command to clear counters of packets matching ACLs.

clear counters access-list [*id* | *name*]

Parameter Description

Parameter	Description
id	Access list number
name	Access list name

Defaults

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the counters of packets matching the specified or all ACLs.

Configuration Examples The following example clears the packet matching counter of ACL No. 2700:

```
Hostname #show access-lists 2700
expert access-list extended 2700
   10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any  (88 matches)
   20 deny tcp any any eq login any any (33455 matches)
   30 permit tcp any any host 192.168.6.9 any (10 matches)

Hostname# clear counters access-list 2700
Hostname #show access-lists 2700
expert access-list extended 2700
   10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
   20 deny tcp any any eq login any any
   30 permit tcp any any host 192.168.6.9 any
```

Related Commands

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Platform Description N/A

1.6 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

1. Standard IP ACL

[*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*] [**log**]

2. Extended IP ACL

- Add a rule of deny type to an IP extended ACL.

[*sn*] **deny** *protocol* { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- Remove a rule of deny type from an IP extended ACL.

no { *sn* | { **deny** *protocol* { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**] } }

Extended IP ACLs of some important protocols:

- Internet Control Message Prot (ICMP)

[*sn*] **deny icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]

- Transmission Control Protocol (TCP)

[*sn*] **deny tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator*[*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

- User Datagram Protocol (UDP)

[*sn*] **deny udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

3. Extended MAC ACL

- Add a rule of deny type to an extended MAC ACL.

[*sn*] **deny** { **any** | **host** *source-mac-address* } { **any** | **host** *destination-mac-address* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*]

- Remove a rule of deny type from an extended MAC ACL.

no { *sn* | {**deny** { **any** | **host** *source-mac-address* } { **any** | **host** *destination-mac-address*} [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*] } }

4. Extended expert ACL

- Add a rule of deny type to an extended expert ACL.

[*sn*] **deny**[*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- Remove a rule of deny type from an extended expert ACL.

no { *sn* | { **deny** [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] } }

- When you select the ethernet-type field or cos field:

[*sn*] **deny** { [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] } [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

- When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destinationdestination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- Extended expert ACLs of some important protocols

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **host** *source-mac-address* | **any** } [*operator* [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **deny udp** [**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **deny arp** [**VID** [*out*] [**inner** *in*]] [*source-mac-address source-wildcard* **| host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] [**time-range** *time-range-name*]

5. Extended IPv6 ACL

- Add a rule of deny type to an extended IPv6 ACL.

[*sn*] **deny** *ipv6*-**protocol** { *source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix/prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]

- Remove a rule of deny type from an extended IPv6 ACL.

no {*sn* | { **deny** *ipv6*-**protocol** { *source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix / prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Extended ipv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** { *source-ipv6-prefix/prefix-length* | *any source-ipv6-address* | **host** } { *destination-ipv6-prefix*/*prefix-length* | **host** *destination-ipv6-address* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** { *source-ipv6-prefix / prefix-length* | **host***source-ipv6-address* | **any** } [*operator* **port** [*port*]] { *destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any** } [*operator* [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

User Datagram Protocol (UDP)

[sn] **deny udp** { *source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any** } [*operator* **port** [*port*]] { *destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any** } [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

Parameter	Description
sn	ACL entry sequence number
source	Source IP address (host address or network address)
source-wildcard	Wildcard masks of a source IP address. The wildcard mask can be discontinuous. For example, 0.255.0.32.
protocol	IP protocol ID. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP and IP or a number representing IP protocols in the range from 0 to 255. Important protocols such as ICMP, TCP and UDP are listed separately for description.
destination	Destination IP address (host address or network address)
destination-wildcard	Wildcard masks of a destination IP address. The wildcard mask can be discontinuous. For example, 0.255.0.32.
fragment	Packet fragment filtering.
precedence	Packet priority.
precedence	The value of packet priority in the range from 0 to 7.
range	The range of Layer 4 port numbers of packets.
lower	The lower limit of the range of Layer 4 port numbers.
upper	The upper limit of the range of Layer 4 port numbers.
tos	Type of service (ToS) in packets.
tos	The value of ToS in the range from 0 to 15.
icmp-type	ICMP message type. The value range is from 0 to 255.
icmp-code	The code of ICMP message type. The value range is from 0 to 255.
icmp-message	Name of ICMP message type.
operator	Operator. (lt: less than. eq: equal to. gt: greater than. neq: not equal to. range: range.)
port	Port number. *range* needs two port numbers and other operators only need one.
host *source-mac-address*	The source MAC address of the host.
host *destination-mac-address*	The destination MAC address of the host.
VID *vid*	Matches specified VIDs.
ethernet-type	Type of an Ethernet protocol.
match-all	Matches all the bits of a TCP flag.
tcp-flag	Mark of a TCP flag.
established	Only matches the RST or ACK bit of a TCP flag.
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point

dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
ipv6-protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the range 0 to 255

Defaults No entry

Command mode ACL configuration mode.

Usage Guide Use this command to configure the filtering entry of ACLs in ACL configuration mode.

Configuration Examples The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
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
Hostname(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Hostname(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)# ip access-list extended ip-ext-acl
Hostname(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)#exit
Hostname(config)#interface gigabitethernet 1/1
Hostname(config-if)#ip access-group ip-ext-acl in
Hostname(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#mac access-list extended mac1
Hostname(config-mac-nacl)#deny host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)# show access-lists
mac access-list extended mac1
```

```
10 deny host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)#exit
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#ip access-list standard 34
Hostname(config-ext-nacl)# deny host 192.168.4.12
Hostname(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Hostname(config-ext-nacl)#exit
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#ipv6 access-list extended v6-acl
Hostname(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
Hostname(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
Hostname(config-ipv6-nacl)# exit
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.
ipv6 traffic-filter	Applies the extended IPv6 ACL on the interface.
ip access-group	Applies the IP ACL on the interface.
mac access-group	Applies the extended MAC ACL on the interface.
ip access-list	Defines an IP ACL.
mac access-list	Defines an extended MAC ACL.
expert access-list	Defines an extended expert ACL.
ipv6 access-list	Defines an extended IPv6 ACL.
permit	Permits the access.

Platform Description N/A

1.7 expert access-group

Use this command to apply the specified expert access list on the specified interface. Use the **no** form of the command to remove the application.

expert access-group { *id* | *name* } **in**

no expert access-group { *id* | *name* } **in**

Parameter Description

Parameter	Description
id	Expert access list number: 2700 to 2899
name	Name of the expert access list
in	Specifies filtering on inbound packets.

Defaults No expert access list is applied on the interface.

Command mode Interface configuration mode.

Usage Guide This command is used to apply the specified access list on the interface to control the input and output data streams. Use the **show access-group** command to view the setting.

Configuration Examples The following example shows how to apply the **access-list *accept***_00d0f8xxxxxx only to Gigabit interface 0/1:

```
Hostname(config)# interface GigaEthernet 0/1
Hostname(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

Related Commands

Command	Description
show access-group	Displays the ACL configuration.

Platform Description N/A

1.8 expert access-list advanced

Use this command to create an advanced expert access list and place the device in expert advanced access list configuration mode. Use the **no** form of this command to remove the advanced expert access list.

expert access-list advanced *name*

no expert access-list advanced *name*

Parameter

Parameter	Description

Description

name	Name of the advanced expert access list

Defaults N/A

Command mode Global configuration mode

Usage Guide Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.

Configuration Examples The following example creates an advanced expert access list named adv-acl.

```
Hostname(config)# expert access-list advanced adv-acl
Hostname(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
show access-lists *name*	Displays the access list of a specified name.

Platform Description N/A

1.9 expert access-list counter

Use this command to enable the counter of packets matching the specified expert access list. Use the **no** form of this command to disable this function.

expert access-list counter { *id* | *name* }

no expert access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	Expert access list number: 2700 to 2899.
name	Name of the access list.

Defaults The counter of the packets matching the expert access list is disabled.

Command mode Global configuration mode

Usage Guide Use this command to enable the counter of packets matching the specified expert access list, so that you can analyze the counters to learn whether the network is attacked by the illegal packets.

Configuration Examples The following example enables the counter of packets matching the extended expert access list named exp-acl:

```
Hostname(config)# expert access-list counter exp-acl
Hostname(config)# show access-lists
expert access-list extended exp-acl
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches)
 20 deny tcp any any eq login any any (78 matches)
```

The following example disables the counter of packets matching the extended expert access list named exp-acl.

```
Hostname(config)#no expert access-list counter exp-acl
Hostname(config)# show access-lists
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
```

Related Commands

Command	Description
show access-lists	Displays the extended expert ACL.

Platform Description N/A

1.10 expert access-list extended

Use this command to create an extended expert access list. Use the **no** form of the command to remove the ACL.

expert access-list extended {*id* | *name*}

no expert access-list extended {*id* | *name*}

Parameter Description

Parameter	Description
id	Extended expert access list number: 2700 to 2899
name	Name of the extended expert access list

Defaults N/A

Command mode Global configuration mode.

Usage Guide Use the **show access-lists** command to display the ACL configurations**.**

Configuration Create an extended expert ACL named exp-acl:

Examples

```
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)# show access-lists expert access-list extended
exp-acl
Hostname(config-exp-nacl)#
```

Create an extended expert ACL numbered 2704:

```
Hostname(config)# expert access-list extended 2704
Hostname(config-exp-nacl)# show access-lists  access-list extended 2704
Hostname(config-exp-nacl)#
```

Related Commands

Command	Description
show access-lists	Displays the extended expert ACLs

Platform Description N/A

1.11 expert access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

expert access-list new-fragment-mode { *id* **|** *name* }

no expert access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	Expert access list number: 2700 to 2899.
name	Name of the expert access list.

Defaults Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode Global configuration mode

Usage Guide Use this command to switch and control the matching mode of access rules to fragmentation packets.

Configuration Examples The following example switches the matching mode of fragmentation packets for the ACL 2700 from the default mode to a new matching mode:

```
Hostname(config)#expert access-list new-fragment-mode 2700
```

Related Commands

Command	Description

-	-

Platform Description N/A

1.12 expert access-list resequence

Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.

expert access-list resequence { *id* | *name* } *start-sn inc-sn*

no expert access-list resequence { *id* | *name* }

Parameter Description

Parameter	Description
Id	Expert access list number: 2700 to 2899.
name	Name of the expert access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults *start-sn*: 10

inc-sn: 10

Command mode Global configuration mode

Usage Guide Use this command to change the order of the access entries.

Configuration Examples The following example resequences entries of expert access list “exp-acl”:

Before the configuration:

```
Hostname# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

After the configuration:

```
Hostname# config
Hostname(config)# expert access-list resequence exp-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

Related

Command	Description

Commands

show access-lists	Displays all access lists..

Platform Description N/A

1.13 global ip access-group

Use this command to apply the global IP-based access list on the interface. Use the **no** form of this command to remove the global IP-based access list from the interface.

global ip access-group

no global ip access-group

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the global IP-based access list is applied on the interface.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example applies the global IP-based access list on interface fastEthernet0/0.

```
Hostname(config)# interface fastEthernet 0/0
Hostname(config-if-GigabitEthernet 0/0)#global ip access-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.14 ip access-group

Use this command to apply a specific access list globally or to an interface. Use the **no** form of this command to remove the access list from the interface.

ip access-group { *id* | *name* } **in**

no ip access-group { *id* | *name* } **in**

Parameter Description

Parameter	Description
id	IP access list or extended IP access list number: 1 to 199, 1300 to 2699
name	Name of the IP ACL
in	Filters the incoming packets of the interface.

Defaults No access list is applied globally or on the interface by default.

Command mode Global or interface configuration mode.

Usage Guide Use this command to control access to a specified interface, globally.

Configuration Examples The following example applies the ACL 120 on interface fastEthernet0/0 to filter the incoming packets:

```
Hostname(config)# interface fastEthernet 0/0
Hostname(config-if)# ip access-group 120 in
```

Related Commands

Command	Description
access-list	Defines an ACL.
show access-lists	Displays all ACLs.

Platform Description N/A

1.15 ip access-list

Use this command to create a standard IP access list or extended IP access list. Use the **no** form of the command to remove the access list.

ip access-list {**extended** | **standard**} {*id* | *name*}

no ip access-list {**extended** | **standard**} {*id* | *name*}

Parameter Description

Parameter	Description
id	Access list number: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
name	Name of the access list

Defaults N/A

Command mode Global configuration mode

Usage Guide Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list.
Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations**.**

Configuration Examples The following example creates a standard access list named std-acl.

```
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)# show access-lists
ip access-list standard std-acl
Hostname(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
Hostname(config)# ip access-list extended 123
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 123
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.

Platform Description N/A

1.16 ip access-list counter

Use this command to enable the counter of packets matching the standard or extended IP access list.
Use the **no** form of this command to disable the counter.
ip access-list counter { *id* | *name* }
no ip access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the IP access list.

Defaults The counter of packets matching the standard or extended IP access list is disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the counter of packets matching the standard access list:

```
Hostname(config)# ip access-list counter std-acl
Hostname(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
 20 deny host 5.5.5.5 time-range tm (2000 matches)
```

The following example disables the counter of packets matching the standard access list:

```
Hostname(config)#no ip access-list counter std-acl
Hostname(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255
 20 deny host 5.5.5.5 time-range tm
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description N/A

1.17 ip access-list log-update interval

Use this command to configure the interval at which the IPv4 access list log is updated. Use the **no** form of this command to restore the default interval.

ip access-list log-update interval *time*

no ip access-list log-update interval

Parameter Description

Parameter	Description
time	For the access rule with the **log** option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults The default interval at which the IPv4 access list log is updated is 5 minutes.

Command mode Global configuration mode

Usage Guide Use this command to configure the interval at which the IPv4 access list log is updated.

Configuration Examples The following example configures the interval for the IPv4 access list log update to 10 minutes:

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# ip access-list log-update interval 10
```

Related Commands

Command	Description
ip access-list	Defines an IPv4 access list.
deny	Defines the **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays running configurations of the device.

Platform Description N/A

1.18 ip access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets of standard or extended IP access list. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

ip access-list new-fragment-mode { *id* **|** *name* }

no ip access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list

Defaults Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode Global configuration mode

Usage Guide This command is used to switch and control the fragmentation packet matching mode of access rules.

Configuration Examples The following example switches the fragmentation packet matching mode of the ACL 100 from the default mode to a new mode:

```
Hostname(config)#ip access-list new-fragment-mode 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.19 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.

ip access-list resequence { *id* | *name* } *start-sn inc-sn*

no ip access-list resequence { *id* | *name* }

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults *start-sn*: 10

inc-sn: 10

Command mode Global configuration mode

Usage Guide Use this command to change the order of the access entries.

Configuration Examples The following example resequences entries of ACL1:

Before the configuration:

```
Hostname# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
Hostname# config
```

```
Hostname(config)# ip access-list resequence 1 21 43
Hostname(config)# exit
Hostname# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description N/A

1.20 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.
ipv6 access-list *name*
no ipv6 access-list *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults N/A

Command mode Global configuration mode

Usage Guide To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the **ipv6 access-list** command.

Configuration Examples The following example creates an IPv6 access list named v6-acl:

```
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
Hostname(config-ipv6-nacl)#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform N/A

Description

1.21 ipv6 access-list counter

Use this command to enable the counter of packets matching the IPv6 access list. Use the **no** form of this command to disable the counter.

ipv6 access-list counter *name*

no ipv6 access-list counter *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults -

Command mode Global configuration mode

Usage Guide Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.

Configuration Examples The following example enables the counter of packets matching the IPv6 access list named v6-acl:

```
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any (7 matches)
 20 deny tcp any any (7 matches)
```

The following example disables the counter of packets matching the IPv6 access list named v6-acl:

```
Hostname(config)#no ipv6 access-list v6-acl counter
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any
20 deny tcp any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description N/A

1.22 ipv6 access-list log-update interval

Use this command to configure the interval at which the IPv6 access list log is updated. Use the **no** form of this command to restore the default interval.

ipv6 access-list log-update interval *time*

no ipv6 access-list log-update interval

Parameter Description

Parameter	Description
time	For the access rule with the **logging** option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults By default, it is 5 minutes.

Command mode Global configuration mode

Usage Guide Use this command to configure the interval at which the IPv6 access list log is updated.

Configuration Examples The following example configures the interval for the IPv6 access list log update to 10 minutes:

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# ipv6 access-list log-update interval 9
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.
deny	Defines the **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays the running configurations of the device.

Platform Description N/A

1.23 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

ipv6 access-list resequence *name start-sn inc-sn*

no ipv6 access-list resequence *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults *start-sn*: 10
inc-sn: 10

Command mode Global configuration mode

Usage Guide Use this command to change the order of the access entries.

Configuration Examples The following example resequences entries of IPv6 access list “v6-acl”:
Before the configuration:

```
Hostname# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

After the configuration:

```
Hostname# config
Hostname(config)# ipv6 access-list resequence v6-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description N/A

1.24 ipv6 traffic-filter

Use this command to apply an IPV6 access list on the specified interface. Use the **no** form of the command to remove the IPv6 access list from the interface/VXLAN.
ipv6 traffic-filter *name* **in**

no ipv6 traffic-filter *name* **in**

Parameter Description

Parameter	Description
name	Name of IPv6 access list
in	Specifies filtering on inbound packets

Defaults By default, it is not disabled.

Command mode Interface configuration mode.

Usage Guide Use this command to apply the IPv6 access list to a specified interface to filter the inbound or outbound packets.

Configuration Examples The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
Hostname(config)# interface GigaEthernet 0/1
Hostname(config-if)# ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-group	Displays ACL configurations on the interface.

Platform Description N/A

1.25 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

list-remark *text*

no list-remark

Parameter Description

Parameter	Description
text	Comment that describes the access list.

Defaults The access lists have no remarks by default.

Command mode ACL configuration mode

Usage Guide You can use this command to write a helpful comment for a specified access list.

Configuration Examples The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

```
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# list-remark this acl is to filter the host
192.168.4.12
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
Hostname(config-ext-nacl)#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IPv4 access list.
access-list list remark	Adds a helpful comment for an access list in global configuration mode.

Platform Description N/A

1.26 mac access-group

Use this command to apply the specified MAC access list on the specified interface. Use the **no** form of the command to remove the access list from the interface.

mac access-group { *id* | *name* } **in**

no mac access-group { *id* | *name* } **in**

Parameter Description

Parameter	Description
id	MAC access list number. The range is from 700 to 799.
name	Name of the MAC access list
in	Specifies filtering on the inbound packets.

Defaults No MAC access list is applied by default.

Command mode Interface configuration mode.

Usage Guide Use this command to apply the access list to the interface to filter the inbound or outbound packets based on the MAC address.

Configuration Examples The following example applies the MAC access-list **accept_00d0f8xxxxxx_only** to interface GigabitEthernet 1/1:

```
Hostname(config)# interface GigaEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# mac access-group
accept_00d0f8xxxxxx_only in
```

Related Commands

Command	Description
show access-group	Displays the ACL configuration on the interface.

Platform Description N/A

1.27 counter

Use this command to enable the counter of packet matching the extended MAC access list. Use the **no** form of this command to disable the counter.

mac access-list counter { *id* | *name* }

no mac access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	Extended MAC access list number. The range is from 700 to 799.
name	Name of the extended MAC access list

Defaults The counter is disabled by default.

Command mode Global configuration mode

Usage Guide Use this command to enable the counter of packets matching the MAC access list to monitor the packets matching and filtering.

Configuration Examples The following example enables the counter of packet matching the extended MAC access list named mac-acl:

```
Hostname(config)# mac access-list counter mac-acl
Hostname(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any (170 matches)
 20 deny any any etype-any cos 6 (239 matches)
```

The following example disables the counter of packet matching the extended MAC access list named mac-acl:

```
Hostname(config)#no mac access-list counter mac-acl
Hostname(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any
```

```
20 deny any any etype-any cos 6
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description N/A

1.28 mac access-list extended

Use this command to create an extended MAC access list. Use the **no** form of the command to remove the MAC access list.

mac access-list extended { *id* | *name* }

no mac access-list extended { *id* | *name* }

Parameter Description

Parameter	Description
id	Extended MAC access list number. The range is from 700 to 799.
name	Name of the extended MAC access list

Defaults N/A

Command mode Global configuration mode.

Usage Guide To filter the packets based on the MAC address, you need to define a MAC access list by using the **mac access-list extended** command.

Configuration Examples The following command creates an extended MAC access list named mac-acl:

```
Hostname(config)# mac access-list extended mac-acl
Hostname(config-mac-nacl)# show access-lists
mac access-list extended mac-acl
```

The following command creates an extended MAC access list numbered 704:

```
Hostname(config)# mac access-list extended 704
Hostname(config-mac-nacl)# show access-lists
mac access-list extended 704
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform N/A

Description

1.29 mac access-list resequence

Use this command to resequence an extended MAC access list. Use the **no** form of this command to restore the default order of access entries.

mac access-list resequence { *id* | *name* } *start-sn inc-sn*

no mac access-list resequence { *id* | *name* }

Parameter Description

Parameter	Description
id	Extended MAC access list number: 700 to 799.
name	Name of the extended MAC access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

The following example resequences entries of extended MAC access list “mac-acl”:

Before the configuration:

```
Hostname# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

After the configuration:

```
Hostname# config
Hostname(config)# mac access-list resequence exp-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description N/A

1.30 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

1. Standard IP ACL

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

2. Extended IP ACL

- Add a rule of permit type to an extended IP ACL.

[*sn*] **permit protocol** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- Remove a rule of permit type from an extended IP ACL.

no { *sn* | { **permit protocol** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**] } }

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [**operator** [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

3. Extended MAC ACL

- Add a rule of permit type to an extended MAC ACL.

[*sn*] **permit** { **any** | **host** *source-mac-address* | *source-mac-address mask*} { **any** | **host** *destination-mac-address* | *destination -mac-address mask* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*]

- Remove a rule of permit type from an extended MAC ACL.

no { *sn* | { **permit** { **any** | **host** *source-mac-address* | *source-mac-address mask*} { **any** | **host** *destination-mac-address* | *destination -mac-address mask* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*] } }

4. Extended expert ACL

- Add a rule of permit type to an extended expert ACL.

[*sn*] **permit** [**protocol** | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source*-mac-*address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- Remove a rule of permit type from an extended expert ACL.

no { *sn* | { **permit** [**protocol** | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source*-mac-*address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] } }

When you select the Ethernet-type field or cos field:

[*sn*] **permit** { *ethernet-type*| **cos** [*out*] [**inner** *in*] } [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

When you select the protocol field:

[*sn*] **permit protocol** [**VID** [*out*] [**inner** *in*] { *source source-wildcard* | **host** *Source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **host** *source-mac-address* | **any** } [*operator* [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* } *| **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [*operator* [**port**]] [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

5. Advanced expert ACL

- Add a rule of permit type to an advanced expert ACL.

[*sn*] **permit** *hex hex-mask offset*

- Remove a rule of permit type from an advanced expert ACL.

no { *sn* | **permit** *hex hex-mask offset* }

6. Extended IPv6 ACL

- Add a rule of permit type to an extended IPv6 ACL.

[*sn*] **permit** *ipv6*-**protocol** { *source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} { *destination-ipv6-prefix/prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]

- Remove a rule of permit type from an extended IPv6 ACL.

no { *sn* | { **permit** *ipv6*-**protocol** { *source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} { *destination-ipv6-prefix* / *prefix-length* | **any**| *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** { *source-ipv6-prefix/prefix-length* | **any** *source-ipv6-address* | **host**} { *destination-ipv6-prefix*/*prefix-length* | **host** *destination-ipv6-address* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** { *source-ipv6-prefix* / *prefix-length* | **host***source-ipv6-address* | **any** } [*operator* **port** [*port*]] { *destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any** } [*operator* [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** { *source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any** } [*operator* **port** [*port*]] { *destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any** } [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

Parameter	Description
sn	ACL entry sequence number
source	Source IP address (host address or network address)
source-wildcard	Wildcard masks of a source IP address. The wildcard mask can be discontinuous. For example, 0.255.0.32.
protocol	IP protocol ID. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP and IP or a number representing IP protocols in the range from 0 to 255. Important protocols such as ICMP, TCP and UDP are listed separately for description.
destination	Destination IP address (host address or network address)
destination-wildcard	Wildcard masks of a destination IP address. The wildcard mask can be discontinuous. For example, 0.255.0.32.
fragment	Packet fragment filtering.
precedence	Packet priority.
precedence	The value of packet priority in the range from 0 to 7.
range	The range of Layer 4 port numbers of packets.

lower	The lower limit of the range of Layer 4 port numbers.
upper	The upper limit of the range of Layer 4 port numbers.
tos	Type of service (ToS) in packets.
tos	The value of ToS in the range from 0 to 15.
icmp-type	ICMP message type. The value range is from 0 to 255.
icmp-code	The code of ICMP message type. The value range is from 0 to 255.
icmp-message	Name of ICMP message type.
operator	Operator. (lt: less than. eq: equal to. gt: greater than. neq: not equal to. range: range.)
port	Port number. *range* needs two port numbers and other operators only need one.
host *source-mac-address*	The source MAC address of the host.
host *destination-mac-address*	The destination MAC address of the host.
VID *vid*	Matches specified VIDs.
ethernet-type	Type of an Ethernet protocol.
match-all	Matches all the bits of a TCP flag.
tcp-flag	Mark of a TCP flag.
established	Only matches the RST or ACK bit of a TCP flag.
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point
dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
ipv6-protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the range 0 to 255
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.

Defaults N/A

Command mode ACL configuration mode.

Usage Guide Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

Configuration Examples

The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
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
Hostname(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
Hostname(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)#exit
Hostname(config)#interface gigabitethernet 1/1
Hostname(config-if)#ip access-group 102 in
Hostname(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#mac access-list extended 702
Hostname(config-mac-nacl)#permit host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
Hostname(config-mac-nacl)#exit
Hostname(config)#interface gigabitethernet 1/1
Hostname(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#ip access-list standard std-acl
Hostname(config-std-nacl)#permit host 192.168.4.12
Hostname(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
```

```
Hostname(config-std-nacl)#exit
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Hostname(config)#ipv6 access-list extended v6-acl
Hostname(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
Hostname(config-ipv6-nacl)# exit
Hostname(config)#interface gigabitethernet 1/1
Hostname(config-if)#ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ipv6 traffic-filter	Applies the extended IPv6 access list to the interface.
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the extended MAC access list to the interface.
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Define an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.
deny	Defines the **deny** access entry.

Platform Description N/A

1.31 redirect destination interface

Use this command to redirect the traffic matching the access list to the specified interface. Use the **no** form of this command to remove the redirection.

redirect destination interface *interface-name* **acl** { *id* | *name* } **in**

no redirect destination interface *interface-name* **acl** { *id* | *name* } **in**

Parameter Description

Parameter	Description
interface-name	Redirect interface
id	Access list number

name	Access list name

Defaults No redirection is configured.

Command mode Interface configuration mode

Usage Guide Use this command to configure access redirection, namely, to redirect the traffic matching the access list to the specified interface. You can monitor the operation of a specified access list by using this command.

Configuration Examples The following example configures access redirection.

```
Hostname(config)# interface gigabitEthernet 0/3
Hostname(config-if-GigabitEthernet 0/3)# redirect destination interface
gigabitEthernet 0/2 acl1 in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.32 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

[sn] **remark** *text*

no *[sn]* **remark**

Parameter Description

Parameter	Description
text	Comment that describes the access entry.
sn	Indicates the sequence number of an ACE comment.

Defaults The access entries have no remarks.

Command mode ACL configuration mode.

Usage Guide Use this command to write a helpful comment for an access entry.

Up to 100 characters are allowed in the remark.

Two access entry remarks in one access list are not allowed.
Removing an access entry may delete the remark for it as well.
If the sn is specified, the comment will match a specified ACE; if no, the comment will match the last ACE in the ACL.

Configuration Examples The following example writes remarks for the entry in extended IP access list 102.

```
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# remark first_remark
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 second_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)# end
Hostname#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IP access list.

Platform Description N/A

1.33 security access-group

Use this command to configure an interface secure channel.
security access-group { *id* | *name* }
no security access-group

Parameter Description

Parameter	Description
id	Access list number.
name	Name of the access list.

Defaults N/A

Command mode Interface configuration mode

Usage Guide If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.

Configuration The following example configures a secure channel on interface GigaEthernet 1/1:

Examples

```
Hostname(config)# interface GigaEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# security access-group 1
```

Related Commands

Command	Description
show secu-acl	Displays the secure channel configuration.

Platform Description N/A

1.34 security global access-group

Use this command to configure the global secure channel.

security global access-group { *id* | *name* }

no security global access-group

Parameter Description

Parameter	Description
id	Access list number.
name	Name of the access list.

Defaults -

Command mode Global configuration mode

Usage Guide If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.

Configuration Examples

```
The following example configures a global secure channel.
Hostname(config)#security global access-group 1
```

Related Commands

Command	Description
show secu-acl	Displays the secure channel configuration..

Platform Description N/A

1.35 security uplink enable

Use this command to configure an exceptional interface of the global secure channel.

security uplink enable
no security uplink enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The global secure channel takes effect on all interfaces by default.

Command mode Interface configuration mode.

Usage Guide The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can used this command to configure the interface as exceptional.

Configuration Examples The following example configures interface GigaEthernet 1/1 as an exceptional interface of the secure channel.

```
Hostname(config)# interface GigaEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# security uplink enable
```

Related Commands

Command	Description
show secu-acl	Displays the secure channel configuration.

Platform Description N/A

1.36 show access-group

Use this command to display the access list applied to the interface.
show access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface	Interface name

Command mode Privileged EXEC mode

Usage Guide Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.

Configuration Examples

```
Hostname# show access-group interface GigabitEthernet 0/3
ip access-list extended 101
```

```
Applied On interface GigabitEthernet 0/3 in.
```

Related Commands

Command	Description
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the MAC access list to the interface.
expert access-group	Applies the expert access list to the interface.
ipv6 traffic-filter	Applies the IPv6 access list to the interface.

Platform Description N/A

1.37 show access-lists

Use this command to display all access lists or the specified access list.

show access-lists [*id* | *name*] [**summary**]

Parameter Description

Parameter	Description
id	Access list number
name	Name of the IP access list
summary	Access list summary

Command mode Global configuration mode

Usage Guide Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

Configuration Examples

```
Hostname# show access-lists n_acl
ip access-list standard n_acl
Hostname# show access-lists 102
ip access-list extended 102

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)
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Defines an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.

Platform Description N/A

1.38 show expert access-group

Use this command to display the expert access list applied to the interface.

show expert access-group [**interface** *interface*]]

Parameter Description

Parameter	Description
interface	Interface name
wlan-id	WLAN ID

Command mode Privileged EXEC mode

Usage Guide Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.

Configuration Examples

```
Hostname# show expert access-group interface gigabitethernet 0/2
expert access-group ee in
Applied On interface GigabitEthernet 0/2.
```

Related Commands

Command	Description
expert access-list	Defines an extended expert access list.

Platform Description N/A

1.39 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

show ip access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface name

Command mode Privileged EXEC mode

Usage Guide Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

Configuration Examples

```
Hostname# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.

Platform Description N/A

1.40 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.
show ipv6 traffic-filter [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface name

Defaults -

Command mode Privileged EXEC mode

Usage Guide Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

Configuration Examples

```
Hostname# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

Related

Command	Description

Commands

ipv6 access-list	Defines an IPv6 access list.

Platform Description N/A

1.41 show mac access-group

Use this command to display the MAC access list on the interface.

show mac access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface name

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.

Configuration Examples

```
Hostname# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

Related Commands

Command	Description
mac access-list	Defines a MAC access list.

Platform Description N/A

1.42 show redirect interface

Use this command to display the access redirection configuration.

show redirect [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to display the access redirection configuration on the interface. If no interface is specified, the access redirection configuration on all interfaces is displayed.

Configuration Examples The following example displays the access redirection configuration on interface GigabitEthernet 0/3.

```
Hostname #show redirect interface gigabitEthernet 0/3
acl redirect configuration on interface gigabitEthernet 0/3
redirect destination interface gigabitEthernet 0/3 acl 1 in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.43 svi router-acls enable

Use this command to enable the SVI filter only for the Layer3 packets. Use the **no** form of this command to disable this function.

svi router-acls enable

no svi router-acls enable

Parameter Description

Parameter	Description
N/A	N/A.

Defaults The SVI filter takes effect for both Layer2 and Layer3 packets by default.

Command mode Global configuration mode

Usage Guide Use this command to make the SVI filter take effect only for the Layer3 packets,

Configuration Examples The following example enables the SVI filter only for the Layer3 packets.

```
Hostname(config)#svi router-acls enable
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

2 QoS Commands

2.1 class

Use this command to add reference to an existing class map. Use the **no** form of this command to remove the class from the policy map.

class *class-map-name*

no class *class-map-name*

Parameter Description

Parameter	Description
class-map-name	Reference to a class map.

Defaults The function is disabled by default.

Command Mode Policy configuration mode

Usage Guide N/A

Configuration Examples The following example adds reference to the class map named cmap1.

```
Hostname(config)# class-map cmap1
Hostname(config-cmap)# match ip dscp 5
Hostname(config-cmap)# exit
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cmap1
Hostname(config-pmap-c)# end
```

Related Commands

Command	Description
show policy-map [*policy-map-name* **[class** *class-map-name*]]	Displays the policy map.

Platform Description N/A

2.2 class map

Use this command to create a class map and enter class-map configuration mode. Use the **no** or **default** form of this command to remove a class map.

class-map *class-map-name*
no class-map *class-map-name*
default class-map *class-map-name*

Parameter Description

Parameter	Description
class-map-name	Class map name. The class map name can be a maximum of 31 characters.

Defaults None

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example creates a class map named cm_acl to match an access list named me.

```
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
Hostname(config-cmap)# exit
```

The following example creates a class map named cm_dscp to match DHCP 8, 16 and 24.

```
Hostname(config)# class-map cm_dscp
Hostname(config-cmap)# match ip dscp 8 16 24
Hostname(config-cmap)# exit
```

Related Commands

Command	Description
show class-map [*class-map-name*]	Displays the class map.

Platform Description N/A

2.3 drr-queue bandwidth

Use this command to set the DRR queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.
drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth
default drr-queue bandwidth

Parameter Description

Parameter	Description
weight1...weight8	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. The weight range is from 0 to 15.

Defaults The default queue weight ratio is 1:1:1:1:1:1:1:1.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the DRR queue weight ratio to 1:1:1:2:2:4:6:8.

```
Hostname(config)# drr-queue bandwidth 1:1:1:2:2:4:6:8
```

Related Commands

Command	Description
show mls qos queuing	Displays information about the queue.

Platform Description N/A

2.4 match

Use this command to define a match criteria in class map configuration mode. Use the **no** form of this command to remove the match criteria.
match { **access-group** *access_list* | **ip** { **dscp** *dscp-vlaue-list* | **precedence** *pre-vlaue-list* } }
no match { **access-group** *access_list* | **ip** { **dscp** *dscp-vlaue-list* | **precedence** *pre-vlaue-list* } }

Parameter Description

Parameter	Description
access-group *access_list*	Identifies a numbered or named access list as the match criteria.
ip dscp *dscp-vlaue-list*	Identifies DSCP values as the match criteria. Multiple DSCP can be configured. The range is from 0 to 63.
ip precedence *pre-vlaue-list*	Identifies IP precedence values as the match criteria. Multiple IP precedence can be configured. The range is from 0 to 7.

Defaults None

Command Mode Class map configuration mode

Usage Guide N/A

Configuration Examples The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30.

```
Hostname(config)# class-map cmap1

Hostname(config-cmap)# match ip dscp 20 22 24 30
```

Related Commands

Command	Description
show class-map [*class-map-name*]	Displays the class map.

Platform Description N/A

2.5 mls qos cos

Use this command to configure the CoS value of an interface. Use the **no** form of this command to restore the default setting.

mls qos cos *default-cos*

no mls qos cos

Parameter Description

Parameter	Description
default-cos	CoS value of the interface. The range is from 0 to 7.

Defaults The default CoS value is 0.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the default CoS value to 7.

```
Hostname(config)# interface gigabitethernet 1/1

Hostname(config-if)# mls qos cos 7
```

Related Commands

Command	Description
show mls qos interface *interface-id*	Displays information of the specified interface.

Platform Description N/A

2.6 mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** or **default** form of this

command to restore the default CoS-DSCP mapping.

mls qos map cos-dscp *dscp1...dscp8*

no mls qos map cos-dscp

default mls qos map cos-dscp

Parameter Description

Parameter	Description
dscp1...dscp8	Specifies the DSCP value. The range is from 0 to 63.

Defaults By default, the CoS 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

```
Hostname(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34
```

Related Commands

Command	Description
show mls qos maps cos-dscp	Displays the CoS-DSCP mapping.

Platform Description N/A

2.7 mls qos map dscp-cos

Use this command to map the DSCP value to the CoS value. Use the **no** or **default** form of this command to restore the default DSCP-CoS mapping.

mls qos map dscp-cos *dscp-list* **to** *cos*

no mls qos map dscp-cos

default mls qos map dscp-cos

Parameter Description

Parameter	Description
dscp-list	DSCP list. The range is from 0 to 63.
cos	CoS value. The range is from 0 to 7.

Defaults The default DSCP-CoS mapping is listed below:

DSCP 0-7	DSCP 8-15	DSCP 16-23	DSCP 24-31	DSCP 32-39	DSCP 40-47	DSCP 48-55	DSCP 56-63
CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Hostname(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related Commands

Command	Description
show mls qos maps dscp-cos	Displays the DSCP-CoS mapping.

Platform Description N/A

2.8 mls qos map ip-precedence-dscp

Use this command to map the IP precedence to the DSCP value. Use the **no** or **default** form of this command to restore the default IP-precedence to DSCP mapping.

mls qos map ip-precedence-dscp *dscp1 ... dscp8*

no mls qos map ip-precedence-dscp

default mls qos map ip-precedence-dscp

Parameter Description

Parameter	Description
dscp1...dscp8	DSCP list. The range is from 0 to 63.

Defaults By default, the IP precedence 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Hostname(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

Related Commands

Command	Description
show mls qos maps ip-pre-dscp	Displays the IP-precedence to DSCP mapping.

Platform Description N/A

2.9 mls qos scheduler

Use this command to configure the output queue scheduling. Use the **no** or **default** form of this command to restore the default scheduler.

mls qos scheduler [**sp** | **rr** | **wrr** | **drr | wfq**]

no mls qos scheduler

Parameter Description

Parameter	Description
sp	Specifies the absolute priority scheduling.
rr	Specifies the round-robin scheduling.
wrr	Specifies the frame count weighted round-robin scheduling.
drr	Specifies the frame length weighted round-robin scheduling.
wfq	Specifies the weighted fair queuing.

Defaults The default queue scheduling is **wrr**.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the sp scheduling.

```
Hostname(config)# mls qos scheduler sp
```

Related Commands

Command	Description
show mls qos scheduler	Displays the output queue scheduling.

Platform Description N/A

2.10 mls qos trust

Use this command to configure the trust mode on an interface. Use the **no** or **default** form of this command to restore the default setting.

mls qos trust { **cos** | **dscp** | **ip-precedence** }

no mls qos trust

default mls qos trust

Parameter Description

Parameter	Description
cos	Specifies the CoS trust mode.
dscp	Specifies the DSCP trust mode.
ip-precedence	Specifies the IP-PRE trust mode.

Defaults No trust mode is configured by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the CoS trust mode.

```
Hostname(config)# interface gigabitethernet 1/1
Hostname(config-if)# mls qos trust cos
```

Related Commands

Command	Description
show mls qos interface *interface-id*	Displays the specified interface configuration.

Platform Description N/A

2.11 police

Use this command to configure traffic policing for a class map in a policy map. Use the **no** form of this command to remove traffic policing for the class map.

police *rate-bps burst-byte* [**exceed-action** { **drop** | **dscp** *new-dscp* | **cos** *new-cos* [**none-tos**] }]

no police

Parameter Description

Parameter	Description
rate-bps	Bandwidth limit value per second (The unit is KBits). The value range is from 64 to 33,554,432.
burst-byte	Burst traffic limit value (The unit is KBytes). The value range is from 4 to 8,192.
drop	Drops the packet. This is available only when the packet exceeds the bandwidth limit.
dscp *new-dscp*	Modifies the DSCP value of the packet. This is available only when the packet exceeds bandwidth limit. The DSCP value range is from 0 to 63.
cos *new-cos*	Modifies the CoS value of the packet. This is available only when the packet exceeds bandwidth limit. The CoS value range is from 0 to 7.
none-tos	Modifies the CoS value only.

Defaults No traffic policing is configured for the class map by default.

Command Mode Policy map class configuration mode

Usage Guide N/A

Configuration Examples The following example configures traffic policing which modifies the DSCP value of the packet to 16 for class map “cm-acl” in policy map “pmap1”.

```
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cm-acl
Hostname(config-pmap-c)# police 102400 4096 exceed-action dscp 16
```

Related Commands

Command	Description
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration.

Platform Description N/A

2.12 policy map

Use the following command to create a policy map and enter policy map configuration mode. Use the **no** or **default** form of this command to remove the specified policy map.
policy-map *policy-map-name*
no policy-map *policy-map-name*
default policy-map *policy-map-name*

Parameter Description

Parameter	Description
policy-map-name	Policy map name. The policy map name can be a maximum of 31 characters.

Defaults No policy map is configured by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example creates policy map “po”, and then adds a reference to class map “cmap1”. Sets the rate limit value to 10 Mbps, the burst traffic limit value to 256 Kbps, and discard packets which exceed the limit.

```
Hostname(config)# policy-map po
Hostname(config-pmap)# class cmaplHostname(config-pmap-c)# police 10240 256
```

```
exceed-action drop
```

Related Commands	Command	Description
	show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration.

Platform Description N/A

2.13 priority-queue

Use this command to configure the output queue scheduling policy to SP. Use the **no** or **default** form of this command to restore the default queue scheduling policy.

priority-queue

no priority-queue

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The default output queue scheduling policy is WRR.

Command Mode Global configuration mode.

Usage Guide This command shares the same configuration with the **mls qos scheduler sp**. The **show run** command displays this configuration in the **mls qos scheduler sp** item instead of **priority-queue**.

Configuration Examples The following example configures the output queue scheduling policy to SP.

```
Hostname(config)# priority-queue
```

Related Commands	Command	Description
	show mls qos scheduler	Displays the output queue scheduling policy.

Platform Description N/A

2.14 priority-queue cos-map

Use this command to configure the mapping between the CoS value and the queue ID. Use the **no** or **default** form of this command to restore the default CoS mapping to the queue.

priority-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]

no priority-queue cos-map

default priority-queue cos-map

Parameter Description

Parameter	Description
qid	Queue ID. The range is from 1 to 8.
cos0 ... cos7	CoS value. The range is from 0 to 7.

Defaults The default mapping between the CoS value and the queue ID is listed below:

Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7	Queue 8
CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example maps the CoS 3, 5 to the output queue 1.

```
Hostname(config)#priority-queue cos-map 1 3 5
```

Related Commands

Command	Description
show mls qos queuing	Displays the output queues.

Platform Description N/A

2.15 qos queue

Use this command to configure a minimum or maximum of the interface bandwidth to a queue. Use the **no** or **default** form of this command to remove the minimum or maximum of the interface bandwidth.

qos queue *queue-id* **bandwidth** { **minimum** | **maximum** } *bandwidth*

no qos queue *queue-id* **bandwidth** { **minimum** | **maximum** }

default qos queue *queue-id* **bandwidth** { **minimum** | **maximum** }

Parameter Description

Parameter	Description
queue-id	Queue ID. The range is from 1 to 8.
bandwidth { **minimum** | **maximum** } *bandwidth*	Bandwidth value. The value range is from 64 to 1,000,000.

Defaults No minimum or maximum of interface bandwidth to a queue is configured by default.

Command Interface configuration mode

Mode

Usage Guide N/A

Configuration Examples

Related Commands	**Command**	**Description**
	show qos bandwidth [**interfaces** *interface-id*]	Displays the interface bandwidth of the queue.

Platform Description N/A

2.16 rate-limit

Use this command to configure rate limiting on the interface. Use the **no** or **default** form of this command to remove rate limiting from the interface.

rate-limit { input | output } *bps burst-size*

no rate-limit { **input | output** }

default rate-limit { **input | output** }

Parameter Description	**Parameter**	**Description**
	input	Configures input rate limiting.
	output	Configures output rate limiting.
	bps	Bandwidth limit value per second (The unit is KBits). The value range is from 64 to 1,000,000.
	burst-size	Burst traffic limit value (The unit is KBytes). The value range is from 4 to 8,192.

Defaults Rate limiting is not configured by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 256 Kbps.

```
Hostname(config)# interface gigabitethernet 1/3

Hostname(config-if-GigabitEthernet 1/3)# rate-limit input 10240 256
```

Related	**Command**	**Description**

Commands		
	show mls qos rate-limit [**interface** *interface-id*]	Displays the rate limiting configuration of the interface.

Platform Description N/A

2.17 service-policy

Use this command to apply the policy map to the interface, the virtual group or globally. Use the **no** or **default** form of this command to remove the policy map.

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

Parameter	Description
policy-map-name	Policy map name
input	Applies the policy map to the input direction.
output	Applies the policy map to the output direction.

Defaults No policy map is configured on the interface or virtual group by default.

Command Mode Interface configuration mode, and virtual group configuration mode.

Usage Guide N/A

Configuration Examples The following example applies policy map “po” to the input direction of interface GigabitEthernet 1/3.

```
Hostname(config)# interface gigabitethernet 1/3
Hostname(config-if-GigabitEthernet 1/3)# service-policy input po
```

The following example applies policy map “po” to the output direction of virtual group 3.

```
Hostname(config)# virtual-group 3
Hostname(config-VirtualGroup)# service-policy output po
```

Related Commands

Command	Description
show mls qos interface policers	Displays the policy map configuration on the interface.
show mls qos virtual-group policers	Displays the policy map configuration on the virtual group.

Platform Description N/A

2.18 set

Use this command to configure the CoS, DSCP or VID value for the traffic. Use the **no** form of this command to remove the CoS, DSCP or VID value from the traffic.

set { **ip dscp** *new-dscp* | **cos** *new-cos* | **vid** *new-vid* }

no set { **ip dscp** | **cos** | **vid** }

Parameter Description

Parameter	Description
ip dscp *new-dscp*	Configures the DSCP value for the traffic. The range is from 0 to 63.
cos *new-cos*	Configures the CoS value for the traffic. The range is from 0 to 7.
vid *new-vid*	Configures the VID value for the traffic. The range is from 1 to 4094.

Defaults No CoS, DSCP or VID value is configured for the traffic in policy map class mode.

Command Mode Policy map class configuration mode

Usage Guide N/A

Configuration Examples The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”.

```
Hostname(config)# policy-map pmap1
Hostname(config-pmap)# class cmap1
```

The following example modifies the CoS value of the traffic to 3.

```
Hostname(config-pmap-c)# set cos 3
```

Related Commands

Command	Description
show policy-map[*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration on the interface.

Platform Description N/A

2.19 show class-map

Use this command to display the class map.

show class-map [*class-map-name*]

Parameter Description

Parameter	Description
class-map-name	Class map name.

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays all class maps.

```
Hostname# show class-map


Class Map cmap1
  Match ip dscp 20 40
Class Map cmap2
  Match access-group 110
```

The fields in the output of this command are described in the following table.

Field	Description
Class Map	Indicates the class map name.
Match	Indicates the matched rule.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 show mls qos interface

Use this command to display the QoS configuration of the interface.

show mls qos interface { *interface-id* | **policers** }

Parameter Description

Parameter	Description
interface-id	Interface name
policers	Displays the traffic policing configured on the interface.

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the QoS configuration of interface GigabitEthernt 1/3.

```
Hostname# show mls qos interface gigabitethernet 1/3

Interface: GigabitEthernet 0/3

Ratelimit input: 10240 256

Ratelimit output: 51200 4096

Attached input  policy-map: pmap1

Attached output policy-map:

Default trust: dscp

Default cos: 3
```

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
Ratelimit input	Indicates the input rate limit value.
Ratelimit output	Indicates the output rate limit value.
Attached input policy-map	Indicates the input policy map.
Attached output policy-map	Indicates the output policy map.
Default trust	Indicates the trust mode of the interface.
Default cos	Indicates the default CoS value.
Scheduler type	Indicates the scheduling policy of the interface.
Wrr queue bandwidth	Indicates the round robin weight ratio of the WRR scheduling policy.
Drr queue bandwidth	Indicates the round robin weight ratio of the DRR scheduling policy.
Wfq queue bandwidth	Indicates the round robin weight ratio of the WFQ scheduling policy.

The following example displays the QoS configuration of all interfaces.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.21 show mls qos maps

Use this command to display DSCP-CoS mapping, CoS-DSCP mapping and IP-PRE-DSCP mapping.

show mls qos maps { cos-dscp | **dscp-cos** | **ip-prec-dscp** }

Parameter Description

Parameter	Description
cos-dscp	Displays the CoS-DSCP mapping.
dscp-cos	Displays the DSCP-CoS mapping.
ip-prec-dscp	Displays the IP-PRE-DSCP mapping..

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the CoS-DSCP mapping.

```
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
```

The fields in the output of this command are described in the following table.

Field	Description
cos	Indicates the CoS value.
dscp	Indicates the DSCP value mapped .

The following example displays the DSCP- CoS mapping.

```
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
```

The fields in the output of this command are described in the following table.

Field	Description
dscp	Indicates the DSCP value.
cos	Indicates the CoS value mapped .

The following example displays the IP-PRE-DSCP mapping.

```
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
```

The fields in the output of this command are described in the following table.

Field	Description
ip-precedence	Indicates the IP-PRE value.
dscp	Indicates the DSCP value mapped .

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.22 show mls qos queuing

Use this command to display the QoS queuing configuration.

show mls qos queueing

Parameter Description

Parameter	Description

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the QoS queuing configuration.

```
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
```

The fields in the output of this command are described in the following table.

Field	Description
Cos-queue map	Indicates the mapping between the CoS value and the queue ID.
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.
cos	Indicates the CoS value.
qid	Indicates the queue ID.
weights	Indicates the weight value

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.23 show mls qos rate-limit

Use this command to display the rate limiting configuration of the interface.

show mls qos rate-limit [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface name

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration The following example displays the rate limiting configuration of all interfaces.

Examples

```
Hostname# show mls qos rate-limit

Interface: GigabitEthernet 0/1

  rate limit input Kbps = 10240 burst = 256

Interface: GigabitEthernet 0/3

  rate limit output Kbps = 102400 burst = 4096
```

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
rate limit input Kbps = x burst = y	Indicates the input rate limit value, and the input burst traffic limit value.
rate limit output Kbps = x burst = y	Indicates the output rate limit value, and the output burst traffic limit value.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.24 show mls qos scheduler

Use this command to display the queue scheduling policy.

show mls qos scheduler

Parameter Description

Parameter	Description

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the queue scheduling policy.

```
Hostname# show mls qos scheduler

Global Multi-Layer Switching scheduling

 Weighted Round Robin
```

The fields in the output of this command are described in the following table.

Field	Description
Weighted Round Robin	Indicates that the queue scheduling policy is WRR. The other queue scheduling policies are listed as follows: SP: Strict Priority RR: Round Robin DRR: Deficit Round Robin WFQ: Weighted Fair Queue

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.25 show mls qos virtual-group

Use this command to display the policy map configuration on the virtual group.

show mls qos virtual-group { *virtual-group-number* | **policers** }

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.
policers	Displays the policy map configuration on all virtual groups.

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the policy map configuration on all virtual groups.

```
Hostname# show mls qos virtual-group policers

Virtual-group: 1

Attached input policy-map: pmap1

Virtual-group: 20

Attached output policy-map: pmap2
```

The fields in the output of this command are described in the following table.

Field	Description
Virtual-group	Indicates the virtual group number.
Attached input policy-map	Indicates the policy map applied on the input virtual group.
Attached output policy-map	Indicates the policy map applied on the output virtual group.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.26 show policy-map

Use this command to display policy maps.

show policy-map [*policy-map-name* [**class** *class-map-name*]]

Parameter Description

Parameter	Description
policy-map-name	Policy map name
class-map-name	Class map name

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays configuration of policy map “pmap1”.

```
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
```

The fields in the output of this command are described in the following table.

Field	Description
Policy Map	Indicates the policy map name.
Class	Indicates the class map name.
set	Indicates that the DSCP value is modified in this example.
police	Indicates bandwidth limit configuration and the action policy for the violated packets.

The following example displays the action policy for the traffic of class map “cmap1” in policy map “pmap1” .

```
Hostname#show policy-map pmap1 class cmap1

Class cmap1

set ip dscp 16
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.27 show qos bandwidth

Use this command to display the bandwidth configuration.

show qos bandwidth [**interfaces** *interface-id*]

Parameter Description	Parameter	Description
	interface-id	Interface name

Defaults None

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the bandwidth configuration of interface GigabitEthernet 0/1.

```
Hostname# show qos bandwidth interface gigabitEthernet 0/1
```

```
Interface: GigabitEthernet 0/1
 ------------------------------------------------
 queue-id | minimum-bandwidth | maximum-bandwidth
 --------   -----------------   -----------------
       1              5120             10240
       2              2048                 0
       3                 0                 0
       4                 0                 0
       5                 0                 0
       6                 0                 0
       7                 0                 0
       8                 0                 0
 ------------------------------------------------
 Total minimum-bandwidth:                  7168
Total maximum-bandwidth:                 10240
```

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
queue-id	Indicates the queue ID.
minimum-bandwidth	Indicates the minimum bandwidth configuration. The unit is Kbps.
maximum-bandwidth	Indicates the maximum bandwidth configuration. The unit is Kbps.
Total queue minimum-bandwidth Total queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when both unicast and multicast queues are displayed.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 show virtual-group

Use this command to display the member port in the virtual group.

show virtual-group { *virtual-group-number* | **summary** }

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.

summary	Displays the member port in all virtual groups.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the member port in all virtual groups.

```
Hostname# show virtual-group summary

 virtual-group       member

 -------------       ------------------------

 1                 Gi0/1 Gi0/2

 2                 Gi0/0
```

The fields in the output of this command are described in the following table.

Field	Description
virtual-group	Indicates the virtual group number.
member	Indicates the member port in the virtual group.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.29 virtual-group

Use this command to create a virtual group in global configuration mode.
Use this command to configure add an interface to a virtual group in interface configuration mode.
Use the **no** or **default** form of this command to remove a virtual group in global configuration mode.
Use the **no** or **default** form of this command to remove an interface from a virtual group in interface configuration mode.
virtual-group *virtual-group-number*
no virtual-group *virtual-group-number*
default virtual-group *virtual-group-number*

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.

Defaults No virtual group is configured, or no interface is added to a virtual group, by default.

Command Mode Interface configuration mode, global configuration mode.

Usage Guide The member port added to the virtual group must be a physical port or an aggregate port member.

Configuration Examples The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:

```
Hostname(config)# interface gigabitethernet 1/3
Hostname(config-if)# virtual-group 3
```

Related Commands

Command	Description
show virtual-group [*virtual-group-number* | **summary**]	Displays the virtual group configuration.

Platform Description N/A

2.30 wfq-queue bandwidth

Use this command to configure the WFQ queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.
wfq-queue bandwidth *weight1 ... weight8*
no wfq-queue bandwidth
default wfq-queue bandwidth

Parameter Description

Parameter	Description
weight1...weight8	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. The weight range is from 0 to 15.

Defaults The default queue weight ratio is 1:1:1:1:1:1:1:1.

Command Mode Global configuration mode.

Usage Guide If the weight value is 0, the SP scheduling policy is applied.

Configuration Examples The following example configures the WFQ queue weight ratio to 1:1:2:4:4:4:6:8.

```
Hostname(config)# wfq-queue bandwidth 1 1 2 4 4 4 6 8
```

Related Commands	Command	Description
	show mls qos queueing	Displays the QoS queuing configuration.

Platform Description N/A

2.31 wrr-queue bandwidth

Use this command to set the WRR weight ratio. Use the **no** or **default** form of this command to restore the default setting.

wrr-queue bandwidth *weight1 ... weight8*

no wrr-queue bandwidth

default wrr-queue bandwidth

Parameter Description	Parameter	Description
	weight1...weight8	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. The weight range is from 0 to 15.

Defaults The default queue weight ratio is 1:1:1:1:1:1:1:1.

Command Mode Global configuration mode

Usage Guide If the weight value is 0, the SP scheduling policy is applied.

Configuration Examples The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.

```
Hostname(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8
```

Related Commands	Command	Description
	show mls qos queuing	Displays the QoS queuing configuration.

Platform Description N/A

Reliability Configuration Commands

1. RLDP Commands

1 RLDP Commands

1.1 rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form of this command to restore the default value.

rldp detect-interval *interval*

no rldp detect-interval

Parameter Description

Parameter	Description
interval	Detection interval in the range 1 to 15 seconds

Defaults 3 seconds.

Command Mode Global configuration mode.

Usage Guide In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

Configuration Examples The following example shows how to set the detection interval as 5s:

```
Hostname(config)# rldp detect-interval 5
```

Related Commands

Command	Description
rldp detect-max	Sets the maximum number of detections.

Platform Description N/A.

1.2 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form of this command to restore it to the default value.

rldp detect-max *num*

no rldp detect-max

Parameter Description

Parameter	Description

num	Maximum number of detections in the range 2 to 10

Defaults 2.

Command Mode Global configuration mode.

Usage Guide This command is used together with the detection interval to specify the maximum number of detections.

Configuration Examples The following example shows how to set the maximum number of detections as 5:

```
Hostname(config)# rldp detect-max 5
```

Related Commands

Command	Description
rldp detect-interval	Sets the detection interval.

Platform Description N/A.

1.3 rldp enable

Use this command to enable RLDP globally. Use the **no** form of this command to disable the function.

rldp enable

no rldp enable

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide You can enable RLDP on the interface only when the global RLDP is enabled.

Configuration Examples The following example shows how to enable RLDP:

```
Hostname(config)# rldp enable
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform Description N/A.

1.4 rldp error-recover interval

Use this command to configure the interval for the RLDP to periodically recover a failed port. Use the **no** form of this command to disable the periodic recovery function. Use the **default** form of this command to restore default settings.

rldp error-recover interval *interval*

no rldp error-recover interval

default rldp error-recover interval

Parameter Description

Parameter	Description
interval	Interval in the unit of seconds, ranging from 30 to 86400.

Defaults This periodic recovery function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Command Mode Global configuration mode

Usage Guide This command is used to automatically and periodically recover a failed RLDP port (in the error state). When the RLDP port recovers from the error, the RLDP on the port restarts link fault detection. If the fault is eliminated, the RLDP maintains the normal state. If the fault persists, the RLDP can still detect the fault.

Configuration Example The following example sets the interval for periodic recovery to 600s.

```
Hostname(config)# rldp error-recover interval 600
```

Prompt N/A

Common Errors N/A

Platform Description N/A

1.5 rldp neighbor-negotiation

Use this command to enable RLDP neighbor negotiation. Use the **no** form or **default** form of this command to restore the default setting.

rldp neighbor-negotiation

no rldp neighbor-negotiation

default rldp neighbor-negotiation

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults RLDP neighbor negotiation is disabled by default.

Command Mode Global configuration mode.

Usage Guide With neighbor negotiation enabled, RLDP unidirectional-/bidirectional-link detection starts only after the neighbor negotiation is successful. (Receiving the Prob message from the neighbor indicates the neighbor negotiation is successful.)

Configuration Examples The following example shows how to enable RLDP neighbor negotiation:

```
Hostname#config
Hostname(config)#rldp neighbor-negotiation
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform Description N/A.

1.6 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

rldp port { **unidirection-detect** | **bidirection-detect** | **loop-detect** } { **warning** | **shutdown-svi** | **shutdown-port** | **block** }

no rldp port { **unidirection-detect** | **bidirection-detect** | **loop-detect | vlan-loop-detect }**

Use this command to enable the VLAN-based loop detection function, and specify the failure treatment.

rldp port vlan-loop-detect { **warning | isolate-vlan** }

Parameter Description

Parameter	Description
unidirection-detect	Sets unidirectional link detection.
bidirection-detect	Sets bidirectional link detection.
loop-detect	Sets loop detection type.
vlan-loop-detect	Sets the VLAN-based loop detection.
warning	Warns the user.
shutdown-svi	Shutdowns the SVI the port belongs to.
shutdown-port	Shutdowns the port.
block	Disables learning and forwarding of a port.
isolate-vlan	Isolates the faulty VLAN.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide The RLDP detection on the port takes effect only when the global RLDP is enabled.

Configuration Examples The following example shows how to enable the RLDP detection and specify the failure treatment as **block**.

```
Hostname(config)# interface GigabitEthernet 2/0/9
Hostname(config-if-GigabitEthernet 2/0/9)# rldp port loop-detect block
```

The following example shows how to configure the VLAN-based loop detection, and specify the failure treatment as **isolate-vlan**.

```
Hostname(config)# interface GigabitEthernet 2/0/10
Hostname(config-if-GigabitEthernet 2/0/10)# switchport mode trunk
Hostname(config-if-GigabitEthernet 2/0/10)# rldp port vlan-loop-detect
isolate-vlan vlan 2-10
```

Related Commands

Command	Description
rldp enable	Enables RLDP globally.

Platform Description N/A.

1.7 rldp reset

Use this command to make all the ports that have been handled using rldp shutdown or disable to perform RLDP detection again.

rldp reset

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The example below demonstrates how to use this command:

```
Hostname# rldp reset
```

Related Commands

Command	Description
rldp enable	Enables RLDP globally.

Platform Description N/A.

1.8 show rldp

Use this command to display the RLDP information.

show rldp [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface ID

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples N/A.

Related Commands

Command	Description

N/A.	N/A.

Platform Description N/A.

Network Management & Monitoring Commands

1. SNMP Commands
2. NTP Commands
3. SPAN-RSPAN Commands
4. sFlow Commands

1 SNMP Commands

1.1 clear snmp locked-ip

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.

clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Parameter Description

Parameter	Description
ipv4 *ipv4-address*	Clears a specified IPv4 address.
ipv6 *ipv6-address*	Clears a specified IPv6 address.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address.

After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.

Configuration Examples The following example clears the whole source IP address table locked after continuous SNMP authentication failures.

```
Hostname#clear snmp locked-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 no snmp-server

Use this command to disable the SNMP agent function.

no snmp-server

Parameter

Parameter	Description

Description

N/A	N/A

Defaults SNMP agent is enabled by default.

Command mode Global configuration mode.

Usage Guide This command disables the SNMP agent services of all versions supported on the device.

Configuration Examples The following example disables the SNMP agent.

```
Hostname(config)# no snmp-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 show snmp

Use this command to display the SNMP configuration.

show snmp [**mib** | **user** | **view** | **group** | **host | locked-ip | process-mib-time**]

Parameter Description

Parameter	Description
mib	Displays the SNMP MIBs supported.
user	Displays the SNMP user information.
view	Displays the SNMP view information.
group	Displays the SNMP user group information.
host	Displays the explicit host configuration.
locked-ip	Displays the source IP addresses locked after continuous SNMP authentication failures.
process-mib-time	Displays the MIB node requiring the longest processing time.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The example below displays the SNMP configuration:

```
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
```

Related Commands

Command	Description
snmp-server chassis-id	Specifies the SNMP system sequence number.

Platform Description N/A

1.4 snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to disable the interface to send link traps.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description
N/A	N/A

Defaults Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

Command mode Interface configuration mode

Usage Guide This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

Configuration Examples The following example disables the interface to send link traps.

```
Hostname(config)# interface gigabitEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Hostname(config)# interface gigabitEthernet 1/1
Hostname(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 snmp-server authentication attempt

Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure. Use the **no** form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.

snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

no snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

Parameter Description

Parameter	Description
times	The maximum number of continuous SNMP authentication failures. The range is from 1 to 10.
exceed	Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded.
lock	Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration.
lock-time *minutes*	Indicates that the source IP address is locked for a period of time. The *minutes* indicates the lock time, ranging from 1 to 65,535. The unit is minute.
unlock	Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed.

Defaults SNMP attack prevention is disabled by default.

Command mode Global configuration mode

Usage Guide The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy.:

1. For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually.
2. For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually.
3. For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.

Configuration Examples The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds.

```
Hostname(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.6 snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

snmp-server chassis-id *text*

no snmp-server chassis-id

Parameter Description

Parameter	Description
text	SNMP chassis ID: numerals or characters.

Defaults The default is 60FF60.

Command mode Global configuration mode.

Usage Guide The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

Configuration Examples The following example specifies the SNMP chassis ID as 123456:

```
Hostname(config)# snmp-server chassis-id 123456
```

Related Commands

Command	Description
show snmp	Displays the SNMP configuration.

Platform Description N/A

1.7 snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

snmp-server community [0 | 7] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [**ipv6** *ipv6-aclname*] [*aclnum*] [*aclname*]

no snmp-server community [0 | 7] *string*

Parameter Description

Parameter	Description
0	Indicates that the community string is in plaintext.
7	Indicates that the community string is in ciphertext.
string	Community string, which is the communication password between the NMS and the SNMP agent
view-name	View name
ro	Indicates that the NMS can only read the variables of the MIB.
rw	Indicates that the NMS can read and write the variables of the MIB.
aclnum	Access list number (1 to 199, and 1300 to 2699), which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Access list name, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6-aclname	IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
ipaddr	Specifies the IP address of the NMS to access the MIB.

Defaults All communities are read only by default.

Command mode Global configuration mode.

Usage Guide This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.

To disable the SNMP agent function, use the **no snmp-server** command.

Configuration Examples The following example defines a SNMP community access string named public, which can be read-only.

```
Hostname(config)# snmp-server community public ro
```

Related Commands

Command	Description
access-list	Defines an access list.

Platform Description N/A

1.8 snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.

snmp-server contact *text*

no snmp-server contact

Parameter Description

Parameter	Description
text	Defines a system contact string.

Defaults No system contact string is set by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the SNMP system contract i-net800@i-net.com.cn:

```
Hostname(config)# snmp-server contact i-net800@i-net.com.cn
```

Related Commands

Command	Description
show snmp-server	Displays the SNMP configuration.
no snmp-server	Disables the SNMP agent function.

Platform Description N/A

1.9 snmp-server enable secret-dictionary-check

Use this command to configure password dictionary checking for communities and users. Use the **no** form of this command to remove the configuration.

snmp-server enable secret-dictionary-check

no snmp-server enable secret-dictionary-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults Password dictionary checking for communities and users is not configured by default.

Command mode Global configuration mode.

Default Level 14

Usage Guide This command must be used together with the **password policy** command in the global configuration mode.

Configuration Examples The following example sets the password length to be no less than six characters and configures password dictionary checking for communities and users.

```
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!
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.10 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap massage to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap massage to NMS.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps

Parameter Description

Parameter	Description
notification-type	Specifies the type of trap messages. snmp: SNMP trap message bridge: Bridge trap message. mac-notification: MAC trap message. ospf: OSPF trap message. vrrp: VRRP trap message. web-auth: Web authentication trap message.

Defaults Sending trap message to the NMS is disabled by default.

Command mode Global configuration mode.

Usage Guide This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

Configuration Examples The following example enables the SNMP agent to send the SNMP trap message.

```
Hostname(config)# snmp-server enable traps snmp
Hostname(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description N/A

1.11 snmp-server enable version

Use this command to enable the functions of Simple Network Management Protocol (SNMP) versions. Use the **no** form of this command to remove the configuration.

snmp-server enable version { **v1** | **v2c** | **v3** }

no snmp-server enable version { **v1** | **v2c** | **v3** }

Parameter Description

Parameter	Description
v1	SNMPv1
v2	SNMPv2c
v3	SNMPv3

Defaults The functions of SNMPv3 are enabled by default.

Command mode Global configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples The following example enables the functions of SNMPv3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable version v3
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.12 snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

snmp-server flow-control pps [*count*]

no snmp-server flow-control pps

Parameter Description

Parameter	Description
count	Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535.

Defaults The default count is 300.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the number of SNMP requests processed per second to 200.

```
Hostname(config)# snmp-server flow-control pps 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.13 snmp-server group

Use this command to configure a new SNMP group**.** Use the **no** form of this command to remove a specified SNMP group.

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [**ipv6** *ipv6_aclname* | *aclnum* | *aclname* }]

no snmp-server group *groupname* {**v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

Parameter Description

Parameter	Description
v1 | **v2c** | **v3**	Specifies the SNMP version
auth	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
noauth	Specifies no authentication a packet. This applies to SNMPv3 only.
priv	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
readview	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
writeview	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
aclnum	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

Defaults No SNMP groups are configured by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures a new SNMP group.

```
Hostname(config)# snmp-server group mib2user v3 priv read mib2
```

Related Commands

Command	Description
show snmp group	Displays the SNMP group configuration.

Platform Description N/A

1.14 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

snmp-server host{ *host-addr* | **ipv6** *ipv6-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**]] *community-string* [**udp-port** *port-num*] [*notification-type*]

no snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]

Parameter Description

Parameter	Description
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
**trap	informs**	Enables the host to send the SNMP notification as traps or informs.
version	SNMP version: V1, V2C or V3
auth	**noauth**	**priv**	Security level of SNMPv3 users
community-string	Community string or username (SNMPv3 version)
port-num	Port of the SNMP host
notification-type	The type of the SNMP trap message, such as **snmp**. If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.

Defaults No SNMP host is specified by default.

Command Global configuration mode.

mode

Usage Guide This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.
Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured.

Configuration Examples The following example specifies an SNMP host to receive the SNMP event trap:

```
Hostname(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message.

Platform Description N/A

1.15 snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout**.**
Use the **no** form of this command to restore the default settings.
snmp-server inform [**retries** *retry-time* | **timeout** *time*]
no snmp-server inform

Parameter Description

Parameter	Description
retry-num	Specifies the resend times for inform requests, ranging from 0 to 255.
time	Specifies the inform request timeout, ranging from 0 to 21,474,836.

Defaults The default *retry-num* is 3, and the default **timeout** *time* is 15 seconds.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the resend times of inform requests to 5.

```
Hostname(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
Hostname(config)# snmp-server inform timeout 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.16 snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

snmp-server location *text*

no snmp-server location

Parameter Description

Parameter	Description
text	String that describes the system location information.

Defaults No system location string is set by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the system location information:

```
Hostname(config)# snmp-server location start-technology-city 4F of A Buliding
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact information.

Platform Description N/A

1.17 snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no** form of this command to remove the network element coding information.

snmp-server net-id *text*

no snmp-server net-id

Parameter Description

Parameter	Description
text	Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces.

Defaults No network element coding information is configured by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the network element coding text to FZ_CDMA_MSC1.

```
Hostname(config)# snmp-server net-id FZ_CDMA_MSC1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.18 snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the **no** form of this command to restore the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter Description

Parameter	Description
byte-count	Packet size. The range is from 484 to 17,876 bytes

Defaults The default is 1,472 bytes.

Command mode Global configuration mode.

Usage Guide The following example specifies the largest size of SNMP packet as 1,492 bytes:

```
Hostname(config)# snmp-server packetsize 1492
```

Configuration Examples N/A

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of the message queue for each SNMP trap host.

Platform Description N/A

1.19 snmp-server queue-length

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no** form of this command to restore the default value.

snmp-server queue-length *length*

no snmp-server queue-length

Parameter Description

Parameter	Description
length	Queue length. The range is from 1 to 1000.

Defaults The default is 10.

Command mode Global configuration mode.

Usage Guide Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.

Configuration Examples The following example specifies the length of message queue as 100.

```
Hostname(config)# snmp-server queue-length 100
```

Related Commands

Command	Description
snmp-server packetsize	Specifies the largest size of the SNMP packet.

Platform Description N/A

1.20 snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

snmp-server system-shutdown
no snmp-server system-shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults The SNMP message reload function is disabled by default.

Command mode Global configuration mode.

Usage Guide Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

Configuration Examples The following example enables the SNMP message reload function:

```
Hostname(config)# snmp-server system-shutdown
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.21 snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.
snmp-server trap-format private
no snmp-server trap-format private

Parameter Description

Parameter	Description
N/A	N/A

Defaults The private field is not carried in the SNMP trap by default.

Command Mode Global configuration mode.

Default Level 14

Usage Guide Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to TRAP-FORMAT-MIB.mib file.

⚠ This command does not work if the traps are sent with SNMPv1.

Configuration Examples The following example configures the SNMP trap format with the private field.

```
Hostname(config)# snmp-server trap-format private
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.22 snmp-server trap-format device-serial-number

Use this command to configure the SNMP traps with device serial numbers. Use the **no** form of this command to restore the default trap format.

snmp-server trap-format device-serial-number

no snmp-server trap-format device-serial-number

Parameter Description

Parameter	Description
N/A	N/A

Defaults The device serial number is not carried in the SNMP trap by default.

Command Mode Global configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples The following example removes the device serial number from the SNMP trap format.

```
Hostname# configure terminal

Hostname (config)# no snmp-server trap-format device-serial-number
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.23 snmp-server trap-format sysmac

Use this command to configure the SNMP traps with sysmacs. Use the **no** form of this command to restore the default trap format.

snmp-server trap-format sysmac

no snmp-server trap-format sysmac

Parameter Description

Parameter	Description
N/A	N/A

Defaults The sysmac is not carried in the SNMP trap by default.

Command Mode Global configuration mode.

Default Level 14

Usage Guide N/A

Configuration Examples The following example removes the sysmac from the SNMP trap format.

```
Hostname# configure terminal

Hostname (config)# no snmp-server trap-format sysmac
```

Verification N/A

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

1.24 snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter Description

Parameter	Description
interface	Specifies the source interface of the SNMP trap messages.

Defaults By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

Command mode Global configuration mode.

Usage Guide For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.

Configuration Examples The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

```
Hostname(config)# snmp-server trap-source fastethernet 0/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables t the SNMP agent to send the SNMP trap massage to NMS.
snmp-server host	Specifies the NMS host to send the SNMP trap message.

Platform Description N/A

1.25 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000.

Defaults The default is 30 seconds.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the timeout period as 60 seconds.

```
Hostname(config)# snmp-server trap-timeout 60
```

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of message queue for the SNMP trap host.
snmp-server host	Specifies the NMS host to send the SNMP trap message.
snmp-server trap-source	Specifies the source address of the SNMP trap message.

Platform Description N/A

1.26 snmp-server udp-port

Use this command to specify a port to receive SNMP packets**.** Use the **no** form of this command to restore the default setting.

snmp-server udp port *port-number*

no snmp-server udp port

Parameter Description

Parameter	Description
port-number	Specifies a port to receive the SNMP packets.

Defaults The default is 161.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies port 15000 to receive the SNMP packets.

```
Hostname(config)# snmp-server udp-port 15000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.27 snmp-server user

Use this command to configure a new user to an SNMP group**.** Use the **no** form of this command to remove a user from an SNMP group.

snmp-server user *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { [**ipv6** *ipv6_aclname*] [*aclnum* | *aclname* }]]

no snmp-server user *username groupname* { **v1** | **v2c** | **v3** }

Parameter Description

Parameter	Description
username	Name of the user on the host that connects to the agent.
groupname	Name of the group to which the user belongs.
v1 | v2c | v3	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.
encrypted	Specifies whether the password appears in cipher text. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by

	the local SNMP engine on the switch.
auth	Specifies which authentication level should be used.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

Defaults N/A

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Hostname(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

Related Commands

Command	Description
show snmp user	Displays the SNMP user configuration.

Platform Description N/A

1.28 snmp-server view

Use this command to configure an SNMP view**.** Use the **no** form of this command to remove an SNMP view.

snmp-server view *view-name oid-tree* { **include** | **exclude** }

no snmp-server view *view-name* [*oid-tree*]

Parameter Description

Parameter	Description
view-name	View name
oid-tree	Specifies the MIB object to associate with the view.
include	Includes the sub trees of the MIB object in the view.
exclude	Excludes the sub trees of the MIB object from the view.

Defaults By default, a view is set to access all MIB objects.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
Hostname(config)# snmp-server view mib2 1.3.6.1 include
```

Related Commands

Command	Description
show snmp view	Displays the SNMP view configuration.

Platform Description N/A

2 NTP Commands

2.1 no ntp

Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.

no ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults NTP is disabled by default.

Command mode Global configuration mode.

Usage Guide By default, NTP is disabled. However, once the NTP server or the NTP primary clock is configured, the NTP service will be enabled.

Configuration Examples The following example disables NTP.

```
Hostname(config)#no ntp
```

Related Commands

Command	Description
ntp server	Specifies an NTP server.

Platform Description N/A

2.2 ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } { *access-list-number* | *access-list-name* }

no ntp access-group {**peer** | **serve** | **serve-only** | **query-only**} { *access-list-number* | *access-list-name* }

Parameter Description

Parameter	Description
peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.

serve	Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.
serve-only	Allows the device to receive only time requests from the servers specified in the access list.
query-only	Allows the device to receive only NTP control queries from servers specified in the access list.
access-list-number	Access control list number, ranging from 1 to 99 and 1300 to 1999.
access-list-name	Access control list name.

Defaults No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

Command mode Global configuration mode.

Usage Guide Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).
The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: **peer**, **serve**, **serve-only**, **query-only**.
If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

⚠ NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

Configuration Examples The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

```
Hostname(config)# access-list 1 permit 192.168.1.1
Hostname(config)# ntp access-group serve-only 1
```

Related Commands

Command	Description
ip access-list	Creates an IP access control list.

Platform Description N/A

2.3 ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP

authentication.

ntp authenticate

no ntp authenticate

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command mode Global configuration mode.

Usage Guide If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.

NTP authentication is implemented through the trusted key specified by the **ntp authentication-key** and **ntp trusted-key** commands.

Configuration Examples After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

```
Hostname(config)#ntp authentication-key 6 md5 wooooop
Hostname(config)#ntp trusted-key 6
Hostname(config)#ntp authenticate
```

Related Commands

Command	Description
ntp authentication-key	Sets the global authentication key.
ntp trusted-key	Configures the global trusted key.

Platform Description N/A

2.4 ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id*

Parameter Description

Parameter	Description
key-id	Key ID, ranging from 1 to 4294967295.
key-string	Key string.

	An encrypted key supports up to 64 bytes of length, while a non-encrypted key supports up to 31 bytes.
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default.

Defaults NTP authentication key is not configured by default.

Command mode Global configuration mode.

Usage Guide Use this command to configure an NTP authentication key and enables the **md5** algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the **ntp trusted-key** command..
You can configure up to 1024 NTP authentication keys. However, each server can support only one key.

Configuration Examples The following example configures an NTP authentication key.

```
Hostname(config)ntp authentication-key 6 md5 wooooop
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp trusted-key	Configures an NTP trusted key.
ntp server	Specifies an NTP server.

Platform Description N/A

2.5 ntp disable

Use this command to disable the device to receive NTP packets on the specified interface.
ntp disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults All NTP packets can be received by default.

Command mode Interface configuration mode.

Usage Guide The NTP message received on any interface can be provided to the client to carry out the clock

adjustment. The function can be set to shield the NTP message received from the corresponding interface.

By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.


This command is configured only the interface that can receive and send IP packets.

Configuration Examples The following example disables the device to receive the NTP packets.

```
Hostname(config-if)# no ntp disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.6 ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

ntp master [*stratum*]

no ntp master

Parameter Description

Parameter	Description
stratum	Stratum level. The range is from 1 to 15. The default is 8.

Defaults N/A

Command mode Global configuration mode.

Usage Guide In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to t other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.


Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.

Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock source.

Configuration Examples The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
Hostname(config)# ntp master 12
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.7 ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

ntp server { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *if-name*] [**key** *keyid*] [**prefer**]

no ntp server *ip-addr*

Parameter Description

Parameter	Description
ip-addr	Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.
domain	Sets the domain name of the NTP server, supporting IPv4 and IPv6.
version	(Optional) Specifies the NTP version (1-3). The default is NTPv3.
if-name	(Optional) Specifies the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295.
prefer	(Optional) Specifies the given NTP server as the preferred one.

Defaults No NTP server is configured by default.

Command mode Global configuration mode.

Usage Guide At present, the system only supports clients other than servers. Up to 20 servers can be synchronized.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.
In the same condition (for instance, precision), the prefer clock is used for synchronization.

⚠ The source interface of NTP packets must be configured with the IP address and can be communicated with the peer.

Configuration Examples The following example configures an NTP server.
For IPv4: `Hostname(config)# ntp server 192.168.210.222`
For IPv6: `Hostname(config)# ntp server 10::2`

Related Commands

Command	Description
no ntp	Disables NTP.

Platform Description N/A

2.8 ntp service disable

Use this command to disable the NTP service. Use the **no** form of this command to remove the configuration.
ntp service disable
no ntp service disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NTP service is enabled by default.

Command mode Global configuration mode.

Default Level 14

Usage Guide If NTP works in the client or server mode, the device acts as a time server to provide the time synchronization service for other devices after synchronizing time from an external reliable clock source.
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 service cannot be disabled. If this command is configured, the **ntp master** command cannot be configured.

Configuration Examples The following example disables the NTP service.

```
Hostname(config)# ntp service disable
```

Verification Run the **show run | in ntp** command to check NTP configuration.

Prompt Messages N/A

Common Errors N/A

Platform Description N/A

2.9

2.10 ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter Description

Parameter	Description
key-id	Global trusted key ID, ranging from 1 to 4294967295.

Defaults N/A

Command mode Global configuration mode.

Usage Guide The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

Configuration Examples The following example configures an authentication key and sets it as a trusted key.

```
Hostname(config)#ntp authentication-key 6 md5 wooooop
Hostname(config)#ntp trusted-key 6
Hostname(config)#ntp server 192.168.210.222 key 6
```

Related Commands

Command	Description

ntp authenticate	Enables NTP authentication.
ntp authentication-key	Configures an NTP authentication key.
ntp server	Configures an NTP server.

Platform Description N/A

2.11 ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the **no** form of this command to remove this function.

ntp update-calendar

no ntp update-calendar

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, update the calendar periodically is not configured.

Command mode Global configuration mode.

Usage Guide By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

Configuration Examples The following example configures the NTP update calendar periodically.

```
Hostname(config)# ntp update-calendar
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.12 show ntp server

Use this command to display the NTP server configuration.

show ntp server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

Usage Guide N/A

Configuration Examples The following example displays the NTP server.

```
Hostname# show ntp server
ntp-server                              source    keyid       prefer  version
----------------------------------------  --------  -----------  ------
-------
10::2                                  None      None        FALSE   3
192.168.210.222                          None      None        FALSE   3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 show ntp status

Use this command to display the NTP configuration.

show ntp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

Usage Guide Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.

Configuration Examples The following example displays the NTP configuration.

```
Hostname# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC )
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3 SPAN-RSPAN Commands

3.1 mac-loopback

Use this command to enable MAC loopback. Use the **no** form of this command to disable MAC loopback.

mac-loopback

no mac-loopback

Parameter Description

Parameter	Description
N/A	N/A

Defaults MAC loopback is disable by default.

Command mode Interface configuration mode.

Usage Guide The MAC loopback feature must be enabled on the interfaces for purposes of local one-to-many mirroring. (Please enable the MAC loopback feature on the down interface, and do not add other configurations to the interface.)

Configuration Examples The following example configures a remote VLAN.

```
Hostname(config)#vlan 100
Hostname(config-vlan)#remote-span
Hostname(config-vlan)#exit
```

The following example configures a session and specifies the mirrored port.

```
Hostname(config)#monitor session 1 remote-source
Hostname(config)#monitor session 1 source interface gigabitEthernet 4/1 both
```

The following example configures the mirroring port, and enables MAC loopback on the port.

```
Hostname(config)#monitor session 1 destination remote vlan 100 interface
gigabitEthernet 4/2 switch
Hostname(config)#interface gigabitEthernet 4/2
Hostname(config-if-GigabitEthernet 4/2)#switchport access vlan 100
Hostname(config-if-GigabitEthernet 4/2)#mac-loopback
```

The following example adds interfaces GigabitEthernet 4/3-4 to the remote VLAN.

```
Hostname(config)#interface range gigabitEthernet 4/3-4
Hostname(config-if-range)#switchport access vlan 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.2 monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).
monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**]

Use this command to configure the SPAN session and specify the destination port (monitoring port).
monitor session *session-num* **destination interface** *interface-id* [**switch**]

Use this command to configure the remote SPAN session ID on the source device..
monitor session *session-num* **remote-source**

Use this command to configure the remote SPAN session ID on the destination device.
monitor session *session-num* **remote-destination**

Use this command to configure the remote SPAN session and specify the remote SPAN destination VLAN.
monitor session *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id* [**switch**]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.
no monitor session *session-num* [**source interface** *interface-id* | **destination interface** *interface-id*]

Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.
no monitor session *session-num* [**destination remote vlan** *remote-vlan-id* **interface** *interface-id*]

Use this command to remove the specified remote SPAN session, or remote the destination port of the remote SPAN session.
default monitor session *session-num* [**destination remote vlan** *remote-vlan-id* **interface** *interface-id*]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.
default monitor session *session-num* { **source interface** *interface-id* | **destination interface**

interface-id }

Parameter Description

Parameter	Description
session_number	SPAN session number
interface-id	Interface name
remote-vlan-id	Remote VLAN ID
vlan-id	VLAN ID (remote VLAN excluded)
vlan-id-list	VLAN list (remote VLAN excluded)
rx	Monitors the only received traffic.
tx	Monitors the only transmitted traffic.
both	Monitors both received and transmitted traffic. This is the default.
switch	Enables switching on the destination port.

Defaults Port monitoring is disabled by default.

Command mode Global configuration mode.

Usage Guide Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.
If the **both**, **rx** or **tx** is not specified for the source port, the **both** parameter is the default.
Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored.
The **switch** feature is disabled on the destination port.

Configuration Examples The following example configures the source port and destination port of the SPAN session.

```
Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1
Hostname(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

The following example configures a remote SPAN session.

```
Hostname(config)# monitor session 10 remote-source
```

The following example configures the destination port of the remote SPAN session.

```
Hostname(config)# monitor session 4 destination remote vlan 10 interface
gigabitEthernet 0/5
```

The following example removes the SPAN session.

```
Hostname(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
Hostname(config)# no monitor session  1 source interface gigabitEthernet 0/18
Hostname(config)# no monitor session  1 destination interface gigabitEthernet
```

```
0/18
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 remote-span

Use this command to configure a remote SPAN VLAN in VLAN configuration mode. Use the **no** form of this command to disable the remote SPAN VLAN.

remote-span

no remote-span

Parameter Description

Parameter	Description
N/A	N/A

Defaults Remote SPAN VLAN is disabled by default.

Command mode VLAN configuration mode.

Usage Guide N/A

Configuration Examples The following example configures a remote SPAN VLAN.

```
Hostname(config)# vlan 100
Hostname(config-vlan)# remote-span
```

Related Commands

Command	Description
show vlan	Displays VLAN configuration.

Platform Description N/A

3.4 show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Parameter Description

Parameter	Description
session_number	Displays the specified SPAN session.

Defaults N/A

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage Guide N/A

Configuration Examples This following example displays all SPAN sessions.

```
Hostname(config)# show monitor
sess-num: 2
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/5     frame-type Both
dest-intf:
TenGigabitEthernet 0/6
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/3     frame-type Both
dest-intf:
```

The following example displays SPAN session 1.

```
Hostname(config)# show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/3     frame-type Both
dest-intf:
TenGigabitEthernet 0/4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4 sFlow Commands

4.1 sflow agent

Use this command to configure the address of the sFlow Agent.
sflow agent { **address** { *ipv4-address* **| ipv6** *ipv6-address* } } | { **interface** { *interface-name* | **ipv6** *interface-name* } }

Use this command to delete the address of the sFlow Agent.
no sflow agent { address | interface }

Use this command to restore the default setting.
default sflow agent { address | interface }

Parameter Description

Parameter	Description
address	Configures the IP address of the sFlow Agent.
Ipv4-address	sFlow Agent IPv4 address.
ipv6 *ipv6-address*	sFlow Agent IPv6 address.
interface	Configures the interface of the sFlow Agent.
interface-name	Interface of IPv4 address.
ipv6 *interface-name*	Interface of IPv6 address.

Defaults

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to configure the Agent IP address field in the output sFlow datagram. The datagram not configured with this filed cannot be output. The sFlow Agent address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Agent address, a message indicating configuration failure is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.

Configuration Examples The following example configures 192.168.2.1 as the sFlow Agent address.

```
Hostname(config)# sflow agent address 192.168.2.1
```

Verification Use the show sflow command to display the sFlow configuration.

Prompt Prompt an error message when the address is invalid.

Messages `invalid host address.`

Common Errors N/A

Platforms N/A

4.2 sflow collector *collector-id* destination

Use this command to configure the address of the sFlow Collector.
sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6_address* } *udp-port* **]**

Use this command to delete the address of the sFlow Collector.
no sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6_address* } *udp-port* **]**

Use this command to delete the address of the sFlow Collector.
default sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6_address* } *udp-port* **]**

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.
ipv4-address	sFlow Collector IPv4 address
ipv6 *ipv6-address*	sFlow Collector IPv6 address
udp-port	sFlow Collector listening port number

Defaults

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to configure the sFlow Collector address. The sFlow Collector address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Collector address, a message indicating configuration failure is displayed. The sFlow Collector monitors the sFlow datagram on the specified port.

Configuration Examples N/A

Verification Use the **show sflow** command to display the sFlow Collector.

Prompt Messages Prompt an error message when the address is invalid.
`invalid host address.`

No VPN exists.

```
vpn is not exist
```

Common Errors N/A

Platforms N/A

4.3 sflow collector *collector-id* max-datagram-size

Use this command to configure the maximum length of the output sFlow datagram.
sflow collector *collector-id* **max-datagram-size** *datagram-size*

Use this command to restore the default maximum length of the output sFlow datagram.
no sflow collector *collector-id* **max-datagram-size**

Use this command to restore the default maximum length of the output sFlow datagram.
default sflow collector *collector-id* **max-datagram-size**

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.
max-datagram-size *datagram-size*	The maximum length of the output sFlow datagram. The range is from 200 to 9,000.

Defaults The default maximum length of the output sFlow datagram is 1,400.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example configures 1,000 as the maximum length of the output sFlow datagram for sFlow Collector.

```
Hostname(config)# sflow collector 1 max-datagram-size 1000
```

Verification Use the **show sflow** command to display the maximum length of the output sFlow datagram.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.4 sflow counter collector

Use this command to enable the sFlow Agent to send counter samples to the sFlow Collector.
sflow counter collector *collector-id*

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.
no sflow counter collector

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.
default sflow counter collector

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.

Defaults

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command can be used for physical ports and aggregated ports.
sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples The following example enables interface TenGigabitEthernet 0/5 to send counter samples to sFlow Collector 2.

```
Hostname(config-if-TenGigabitEthernet 0/5)# sflow counter collector 2
```

Verification Use the **show sflow** command to display the sFlow counter sampling configuration.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.5 sflow counter interval

Use this command to configure the sFlow counter sampling interval.
sflow counter interval *seconds*

Use this command to restore the default sFlow counter sampling interval.
no sflow counter interval

Use this command to restore the default sFlow counter sampling interval.
default sflow counter interval

Parameter Description

Parameter	Description
seconds	sFlow counter sampling interval. The range is form 3 to 2,147,483,647. The unit is second.

Defaults The default sFLow counter sampling interval is 30 seconds.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.

Configuration Examples The following example configures the sFlow counter sampling interval to 60 seconds.

```
Hostname(config)# sflow counter interval 60
```

Verification Use the **show sflow** command to display the sFlow counter sampling interval.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.6 sflow enable

Use this command to enable flow sampling and counter sampling on the interface.
sflow enable

Use this command to disable flow sampling and counter sampling on the interface.
no sflow enable

Use this command to disable flow sampling and counter sampling on the interface.
default sflow enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The sFlow sampling function on an interface is disabled by default.

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command can be used to enable counter sampling and flow sampling for physical ports and aggregate ports. sFlow datagram can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples The following example enables the sFlow sampling on interface TenGigabitEthernet 0/5.

```
Hostname(config-if-TenGigabitEthernet 0/5)# sflow enable
```

Verification Use the **show sflow** command to display the status of the sFlow sampling function.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.7 sflow flow collector

Use this command to enable the sFlow Agent to send flow samples to the sFlow Collector.
sflow flow collector *collector-id*

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.
no sflow flow collector

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.

default sflow flow collector

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.

Defaults

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command can be used for physical ports and aggregated ports.
sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples The following example enables interface TenGigabitEthernet 0/5 to send flow samples to sFlow Collector 2.

```
Hostname(config-if-TenGigabitEthernet 0/5)# sflow flow collector 2
```

Verification Use the **show sflow** command to display the sFlow flow sampling configuration.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.8 sflow flow max-header

Use this command to configure the maximum length of the packet header copied during flow sampling.
sflow flow max-header *length*

Use this command to restore the default maximum length of the packet header copied during flow sampling.
no sflow flow max-header

Use this command to restore the default maximum length of the packet header copied during flow sampling.
default sflow flow max-header

Parameter Description

Parameter	Description
length	Maximum length of the packet header to be copied. The range is from 18 to 256. The unit is byte.

Defaults The default length is 64 bytes.

Command Mode Global configuration mode

Default Level 14

Usage Guide Configure the maximum number of bytes of the packet content copied from the header of the original packet. The copied content is recorded in the generated sample.

Configuration Examples The following example sets the maximum length of the packet header copied during sFlow flow sampling to 128 bytes.

```
Hostname(config)# sflow flow max-header 128
```

Verification Use the **show sflow** command to display the maximum length of the packet header copied during sFlow flow sampling.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.9 sflow sampling-rate

Use this command to configure the sampling rate of sFlow flow sampling.
sflow sampling-rate *rate*

Use this command to restore the default the sampling rate of sFlow flow sampling.
no sflow sampling-rate

Use this command to restore the default sampling rate of sFlow flow sampling.
default sflow sampling-rate

Parameter Description

Parameter	Description
rate	Sampling rate of sFlow sampling. One packet is sampled from every *n*

	packets (*n* equals the value of rate). The range is from 4,096 to 65,535. The default rate is 8,192.

Defaults The default sFlow flow sampling rate is 8,192.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to configure the global sampling rate of sFlow flow sampling, and sFlow flow sampling of all interfaces uses this sampling rate.

Configuration Examples The following example sets the sFlow flow sampling rate to 4,096.

```
Hostname(config)# sflow sampling-rate 4096
```

Verification Use the **show sflow** command to display the sFlow flow sampling rate.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

4.10 show sflow

Use this command to display the sFlow configuration.

show sflow

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode/global configuration mode/interface configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example displays the sFlow configuration.

```
Hostname(config)#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    Y
TenGigabitEthernet 0/2         0    1    N
```

Field Description:

Field	Description
sFlow datagram version	sFlow datagram version. Currently, pruducts supports V5 only.
Agent IP	IP address of the sFlow Agent. It can be configured by using the sflow Agent address {*ipv4-address* | ipv6 *ipv6-address* } command.
sflow counter interval	Counter sampling interval
sflow flow max-header	The maximum length of bytes of the packet header to be copied
sflow sampling-rate	Flow sampling rate
ID	sFlow Collector ID
IP	The IP address of the sFlow Colletor to receive sFlow datagram
Port	Port No. of the sFlow Collector to receive sFlow datagram
Size	The maximum length of the output sFlow datagram
VPN	VPN instance name of sFlow Collector
Interface	An interface configured with sFlow function
CID	The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.
FID	The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.
Enable	The status of the sFlow sampling function

Prompt Messages N/A

Platforms N/A