NAS Series CLI Manual

Command-line reference for NAS Series switches

GETTING STARTED

Connect your laptop to the switch CLI

Connect over Ethernet using SSH

Use this method when SSH is enabled on the switch and you have a CLI account.

1. Connect the laptop

Connect an Ethernet cable from the laptop to the switch management port, or to a switch port configured for the management VLAN.

2. Set the laptop's Ethernet address

The quick reference gives 192.168.0.1 as the factory management IP. For a direct connection, set the laptop to an unused address such as 192.168.0.2 with subnet mask 255.255.255.0. Leave the gateway blank. If the switch already has a different management IP, use its current subnet.

3. Open an SSH session

Windows: Press Windows key + R, type powershell, then press Enter.

macOS: Press Command + Space, type Terminal, then press Return.

For an authorized CLI account named admin at the factory address, enter:

```
ssh admin@192.168.0.1
```

Substitute your CLI username and the switch's current IP as needed. On first connection, verify the displayed host key fingerprint before accepting it. Enter the CLI password when prompted.

4. Confirm that you are connected

At the switch prompt (for example, Switch> or Switch#), enter the following command to display the switch version:

```
show version
```

Direct access through the console port

If SSH is unavailable, connect a compatible serial console cable from the laptop to the switch port labeled Console. In a serial terminal such as PuTTY, select Serial and the adapter's COM port (Windows Device Manager > Ports). Use the baud rate, data bits, parity, stop bits, and flow control specified for your exact model. Open the session, press Enter, and log in if prompted.

The supplied quick reference documents the web login. It does not specify serial settings, CLI credentials, or whether SSH is enabled at the factory.

Contents

Getting started / Connect your laptop to the switch CLI 2

01 General commands **5**

02 PortCommands **22**

03 Port-based security commands **44**

04 ip mac-bind **48**

05 Port Loop Detection **49**

06 Vlan commands **54**

07 QOS **71**

08 MSTP commands **77**

09 EAPS command **89**

10 ERPS command **95**

11 AAA command **104**

12 GMRP command **116**

13 IGMP SNOOPING command **121**

14 MVR command **129**

15 DHCP SNOOPING **132**

16 DHCP client command **136**

17 DHCP RELAY **138**

18 DHCP SERVER **139**

19 ACL commands **145**

Contents

20	TCP/IP basic commands	**151**
21	SNMP commands	**156**
22	RMON command	**159**
23	Cluster Configuration	**163**
24	SNTP commands	**174**
25	IGMP commands	**177**
26	PIM-SM Command	**183**
27	RIP command	**205**
28	RIPng command	**217**
29	OSPF commands	**225**
30	OSPFv3 commands	**248**
31	BGP Commands	**264**
32	VRRP commands	**288**
33	VLLP commands	**295**
34	Policy Routing Commands	**303**
35	System log commands	**306**
36	IPv6 Commands	**310**
37	MLDsnooping command	**318**
38	POE commands	**324**

CHAPTER 01

General commands

Mode command

configure terminal

Command

```
configure terminal
```

Mode

Privilege mode

Parameters

None.

Description

The configure terminal command is used to enter configuration mode

Examples

Enter global configuration mode:

```
Switch#configure terminal
Switch(config)#
```

disable

Command

```
disable
```

Mode

Privilege mode

Parameters

None

Description

The disable command is used to turn off privileged mode and return to normal mode.

Examples

```
#Close and return to normal mode:
Switch#disable
Switch>
```

enable

Command

```
enable
```

Mode

General mode

Parameters

None

Description

If the password passes, enter privileged mode.

Examples

From normal mode to privileged mode.

```
Switch> enable
password:******
switch#
```

exit

Command

```
exit
```

Mode

All modes

Parameters

None

Description

The exit command is used to end the current mode and return to the previous mode.

Examples

Return from privileged mode to normal mode.

```
Switch#exit
Switch>
```

File management commands

copy running-config startup-config

Command

```
copy running-config startup-config
```

Mode

Privilege mode

Parameters

None.

Description

The copy running-config startup-config command saves the current configuration of the system as a startup configuration file.

Examples

```
#Copy the currently used configuration as the configuration for the next boot.
Switch#copy running-config startup-config
Building and writing configuration ...
Switch#
```

delete startup-config

Command

```
delete startup-config
```

Mode

Privilege mode

Parameters

None.

Description

Delete the boot configuration file. Rebooting the switch after executing this command will restore it to the factory settings.

Examples

Delete startup configuration.

```
Switch#delete startup-config
Switch#
```

download configure

Command

```
download configure <ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: TFTP server ip address.
file-name: The name of the configuration file on the TFTP server.

Description

Download the configuration file from the TFTP server to the switch as the startup configuration file, and the downloaded configuration file takes effect after rebooting the switch.

Examples

```
#Download the configuration file to the host 192.168.0.100. file name is conf.txt:
Switch#download configure 192.168.0.100 conf.txt
```

download switch

Command

```
download switch<ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: The TFTP server ip address.
file-name: the name of the switch file on the TFTP server.

Description

After downloading the switch file, the switch file is written to the switch flash, and the newly downloaded switch file is applied by restarting the switch with the reset command.

Examples

```
#Download switch file from host 192.168.0.100 to the switch:
Switch#download switch192.168.0.100switch.tar.gz
Do you wish to continue?
```

download kernel

Command

```
download kernel<ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: The TFTP server ip address.
file-name: the name of the kernel file on the TFTP server.

Description

Download the kernel file. kernel file will be written to the switch flash after downloading. reboot the switch to apply the newly downloaded kernel file via reset command.

Examples

Download the kernel file from host 192.168.0.100 to the switch:

```
Switch#download switch192.168.0.100kernel
Do you wish to continue?
```

download patch

Command

```
download patch<ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: The TFTP server ip address.
file-name: the name of the kernel file on the TFTP server.

Description

After downloading the patch file, the patch file is written to the switch flash, and the switch is restarted with the reset command to apply the newly downloaded patch file.

Examples

```
#Download the patch file from host 192.168.0.100 to the switch:
Switch#download switch192.168.0.100patch
Do you wish to continue?
```

download uboot

Command

```
download uboot<ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: The TFTP server ip address.
file-name: the name of the kernel file on the TFTP server.

Description

Download the uboot file. uboot file will be written to the switch flash after download, and reboot the switch to apply the newly downloaded uboot file by reset command.

Examples

Download the sdk file from host 192.168.0.100 to the switch:

```
Switch#download switch192.168.0.100 uboot
Do you wish to continue?
```

upload configure

Command

```
upload configure <ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: Indicates the IP address of the destination TFTP server for file uploads.
file-name: the name of the configuration file saved to the TFTP server.

Description

Save the switch's startup configuration file to the TFTP server.

Examples

```
#Save the boot configuration file to the host 192.168.0.100 named conf.
Switch#upload configure 192.168.0.100 conf
```

upload switch

Command

```
upload switch<ip-address><file-name>
```

Mode

Privilege mode

Parameters

ip-address: Indicates the IP address of the destination TFTP server for file uploads.
file-name: the name of the switch file saved to the TFTP server.

Description

Save the switch switch file to TFTP server.

Examples

```
#Save the switch file to the host 192.168.0.100, named switch.
Switch#upload configure 192.168.0.100switch
```

write

Command

```
write
```

Mode

Privilege mode.

Parameters

None.

Description

Save the information of the current user-configured settings.

Examples

```
None.
```

System administration commands

security-manage http

Command

```
security-manage http {access-group <group-id> | disable | enable }
```

Mode

Global configuration mode

Parameters

group-id: the referenced rule group number, rule range <1-99>

Description

Used to set whether web login is supported or not.

Examples

Set up support for logging in as web mode.

```
Switch(config)#security-manage http enable
Switch(config)#
```

security-manage https

Command

```
security-manage https {access-group <group-id> | disable | enable }
```

Mode

Global configuration mode

Parameters

group-id: the referenced rule group number, rule range <1-99>

Description

Used to set whether to support https login.

Examples

Set up support for logging in as https mode.

```
Switch(config)#security-manage https enable
Switch(config)#
```

security-manage snmp

Command

```
security-manage snmp {access-group < group-id> | disable | enable }
```

Mode

Global configuration mode

Parameters

group-id: the referenced rule group number, rule range <1-99>

Description

Used to set whether snmp login is supported or not.

Examples

Set up support for logging in as snmp mode.

```
Switch(config)#security-manage snmp enable
Switch(config)#
```

security-manage telnet

Command

```
security-manage telnet {access-group <group-id> | disable | enable | number <number> }
```

Mode

Global configuration mode

Parameters

group-id: the referenced rule group number, rule range <1-99>
number: the number of telnet logins supported

Description

Used to set whether telnet login is supported or not.

Examples

Set up support for logging in as telnet mode.

```
Switch(config)#security-manage telnet enable
Switch(config)#
```

security-manage ssh

Command

```
security-manage ssh {access-group < group-id> | disable | enable }
```

Mode

Global configuration mode

Parameters

group-id: the referenced rule group number, rule range <1-99>

Description

Used to set whether ssh login is supported or not.

Examples

Set up support for logging in as ssh mode.

```
Switch(config)#security-manage ssh enable
Switch(config)#
```

show security-manage

Command

```
show security-manage
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

The show security-manage command is used to display system security information.

Examples

Display system security management information

```
Switch#show security-manage
Service type    Admin state    Access-list name
------------    -----------    ----------------
http           enable         0
snmp          enable         0
telnet          enable         88
Switch#
```

enable password

Command

```
enable password <password>
no enable password
```

Mode

Global configuration mode

Parameters

password: password string. The default password is empty.

Description

The enable password command is used to modify the password for the switch to enter privileged mode from normal mode.

The no enable password command is used to cancel the password.

Examples

Change the password of the switch to admin.

```
Switch(config)#enable password admin
```

exec-timeout

Command

```
exec-timeout <minutes> [<seconds>]
no exec-timeout
```

Mode

Terminal configuration mode

Parameters

Minutes: minutes, range 0-35791.
seconds: seconds, range 0-59.

Description

The exec-timeout command is used to configure the telnet terminal idle time out. The default value is 10 minutes.
The no exec-timeout command is used to cancel the configuration and restore the default value.

Examples

Configure the timeout to 15 minutes.

```
Switch(config-line)#exec-timeout 15
Switch(config-line)#
```

reset

Command

```
reset
```

Mode

Privilege mode.

Parameters

None.

Description

The reset command is used to reboot the switch.

Examples

```
None.
```

set date-time

Command

```
set date-time <year><month><day><hour><minute><second>
```

Mode

Privilege mode

Parameters

year: Set year, range: 2000-2037.
month: Set the month, range: 1-12.
day: Set the day, range: 1-31.
hour: Set the hour, range: 0-23.
minute: Set the minutes, range: 0-59.
second: Set seconds, range: 0-59.

Description

The set date-time command is used to set the system time.

Examples

```
None.
```

show date-time

Command

```
show date-time
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show date-time command is used to display the current date and time of the system

Examples

```
Switch#show date-time
System Date Time : 2014/2/17 11:27:46
Switch#
```

show history

Command

```
show history
```

Mode

Normal mode / Privilege mode.

Parameters

None.

Description

The show history command is used to display the command history, and can display the 20 commands executed before this command.

Examples

```
None.
```

show version

Command

```
show version
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show version command is used to display system version information.

Examples

Show system version

```
Switch# show version
Product: Switch
Firmware:
Version: 1.3.7 Build time: Oct 11 2019 19:22:04
Uboot:
Version: 1.1.7 Build time: Oct 20 2016 12:00:00
Kernel:
Linux version 3.6.5-Broadcom Linux #55 SMP Mon Jun 17 11:03:58 CST 2019
SDK:
Version: Broadcom SDK 6.3.3 v1.2.4 Build time: Jul 31 2019 13:41:13
```

```
Patch:
Version: 1.0.2
Switch#
```

show switch

Command

```
show switch
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show switch command is used to display the system mac address and serial number.

Examples

Display system mac address and serial number

```
Switch>show switch
MAC address : 00:09:ca:11:11:11
Serial number : s012345678912
Switch>
```

terminal

Command

```
terminal{length <number>|no length}
```

Mode

Normal mode / Privilege mode

Parameters

length: Specifies the number of lines to be displayed to the screen at a time. The default is 25 lines.
no length: Uncomment the number of lines to be displayed.

Description

The terminal command is used to configure the number of lines that the terminal displays to the screen at one time.

Examples

Configure the terminal to display 10 lines at a time:

```
Switch#terminal length 10
```

who

Command

```
who
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The who command is used to display the current user of vty.

Examples

Show current VTY users.

```
Switch#who
vty[0] connected from local
```

View configuration commands

show running-config

Command

```
show running-config [access-list | interface | ip {igmp snooping | route} | key chain | mstp | ospf |
prefix-list | rip | route-map | vlan]
```

Mode

Privilege mode

Parameters

access-list: The relevant configuration of ACLs.
interface: Configuration of the interface, including physical and virtual interfaces.
ip igmp snooping: Configuration related to igmp snooping.
ip route: Routing-related configuration.
key chain: The configuration of the authentication key chain.
mstp: Configuration related to mstp.
ospf: Configuration related to ospf.
prefix-list: configuration related to the prefix list.
rip: Configuration related to the rip protocol.
route-map: Configuration of the routing table.
vlan: Configuration related to vlan.

Description

The show running-config command is used to display the current configuration information.

Examples

```
None.
```

show startup-config

Command

```
show startup-config
```

Mode

Privilege mode

Parameters

None

Description

The show startup-config command is used to display the contents of the system startup configuration file.

Examples

```
None.
```

Mac address table commands

bridge ageing-time

Command

```
bridge ageing-time <time>
no bridge ageing-time
```

Mode

Global configuration mode

Parameters
time: mac table aging time, range: 10-1000000 seconds. Default is 300 seconds.

Description
The bridge ageing-time command is used to set the ageing time of the mac address table.
The nobridge ageing-time command restores the age time of the mac address table to its factory value.

Examples
Set the aging time of the switch to 100 seconds.

```
Switch(config)#bridge ageing-time 100
Switch(config)#
```

bridge address

Command

```
[no] bridge address <mac-address> {discard|forward} <if-name>[vlan <vlan-id>]
```

Mode
Global configuration mode

Parameters
mac-address: mac address, format HHHH.HHHH.
if-name: The specific interface.
vlan-id: vlan number

Description
The bridge address command is used to configure the MAC address of the interface for filtering or forwarding.

Examples

```
#
Switch(config)#bridge address 0000.0001.0001 discard ge1/1
Switch(config)#
```

clear mac address-table dynamic

Command

```
clear mac address-table dynamic
```

Mode
Privilege Mode

Parameters
None.

Description
The clear mac address-table dynamic command removes the Layer 2 table dynamic MAC address.

Examples

```
#Remove layer 2 dynamic mac addresses.
Switch#clear mac address-table dynamic interface
```

Network debugging commands

ping

Command

```
ping <ip-address> [-n <count> | -l <size> | -w <timeout>]*
```

Mode
Privilege mode

Parameters
ip-address: The destination IP address.
-n: The number of requests sent.
-l: The length of the sent packet.
-w: The timeout period in seconds to wait for each response.

Description
ping is a network debugging tool to test whether another host is reachable. For simple applications just enter the IP address of the target host; if you use ping as a diagnostic tool, you can enter more detailed parameters.

Examples
Send 5 request packets to host 172.16.0.1.

```
Switch#ping 172.16.0.1 -n 5
```

trace-route

Command

```
trace-route <ip-address>[-h <maximum-hops> | -j <count><ip-address>* | -w <timeout>]*
```

Mode
Privilege mode

Parameters
ip-address: The destination IP address.
-h: the maximum number of hops.
-j: Source band loose route, enter the number of route hops and the IP address of the associated hop. Multiple IP addresses can be entered repeatedly.
-w: Timeout time (seconds).

Description
traceroute detects the routes through which packets travel from one host to another. For this function only, the user only needs to enter the destination IP address. If it is to be used as a network diagnostic the relevant parameters can be entered.
Traceroute is implemented in such a way that UDP packets with increasing TTL are sent from this host to the destination host. If the TTL is zero, the passing router sends a TTL exhausted, host unreachable ICMP packet; if it reaches the host but the host does not have a port for the UDP packet, the host responds with a port unreachable ICMP packet. traceroute determines whether the destination host is reached based on whether the passing ICMP packet is host unreachable or port unreachable. If it is a host unreachable, the router will print the IP address of the router and continue sending UDP packets with TTL plus 1 until the TTL equals Maxmum time to live. if it is a port unreachable, the destination host will print the IP address of the host and stop sending UDP packets.

Examples

```
#Detects the route traversed with a destination of 192.168.10.2 and a maximum hop count of 10 hops.
Switch#trace-route 192.168.10.2 -n 10
```

telnet

Command

```
telnet <ip-address>
```

Mode
Normal mode / Privilege mode

Parameters
ip-address: The IP address of the target device.

Description
To access other devices remotely through Telnet client , you can press CTRL+] key combination to force quit.

Examples

```
#Login to the device with remote IP 192.168.0.2.
Switch#telnet 192.168.0.2
```

ssh

Command

```
ssh <ip-address> [user-name]
```

Mode

Privilege mode

Parameters

ip-address: The IP address of the target device, supporting ipv4 and ipv6.
user-name: the user name to login to the ssh server, default is admin

Description

Remote access to other devices via ssh client.

Examples

```
#Login to the device with remote IP 192.168.0.2.
Switch#ssh 192.168.0.2
```

Multi-user management commands

username

Command

```
username <username> password <password> {normal | privilege}
no username [username]
```

Mode

Global configuration mode

Parameters

username: username string, maximum length is 64.
password: password string, maximum length is 64.
normal: Normal permission.
privilege: Privileged access.

Description

The username command allows you to add users and change passwords or permissions for users that already exist.
The no username command is used to delete a user or all users that already exist.

Examples

```
#Add a user with username abc, password abc and permission normal.
Switch(config)#username abc password abc normal
Switch(config)#
```

System monitoring commands

show process cpu

Command

```
show process cpu
```

Mode

Privilege mode

Parameters
None

Description
The show process cpu command is used to display the system CPU utilization.

Examples

```
Switch#show process cpu
Switch#
Mem: 66608K used, 171264K free, 0K shrd, 0K buff, 28716K cached
CPU: 0% usr 0% sys 0% nic 55% idle 0% io 0% irq 45% sirq
Load average: 0.16 0.12 0.14 1/57 477
PID PPID USER STAT VSZ %VSZ %CPU COMMAND
430 1 root S 13884 6% 0% /home/bak/switch/app/nsm -d
459 1 root S 3280 1% 0% /home/lighttpd/lighttpd -f /home/light
440 380 root S 2936 1% 0% /home/bak/switch/app/imi -f /home swit
434 1 root S 2876 1% 0% /home/bak/switch/app/mstpd -d
441 1 root S 1948 1% 0% /home/bak/switch/app/ripd -d
444 1 root S 1504 1% 0% /home/snmpd -c /home/snmpd.conf -Le
1 0 root S 1212 1% 0% init
380 378 root S 1204 1% 0% {do} /bin/sh /home/do
378 1 root S 1204 1% 0% {initswitch} /bin/sh /etc/initswitch
477 476 root R 1200 1% 0% top -n 1
476 440 root S 1200 1% 0% /bin/sh -c top -n 1 > /home/monitor/cp
369 1 root S 1196 1% 0% /sbin/klogd
367 1 root S 1196 1% 0% /sbin/syslogd -m 0
452 1 root S 1172 0% 0% /home/bak/switch/app/dropbear
395 2 root SW< 0 0% 0% [bcmL2X.0]
405 2 root SW< 0 0% 0% [bcmCNTR.0]
399 2 root SW< 0 0% 0% [bcmLINK.0]
389 2 root SW< 0 0% 0% [bcm-shell]
319 2 root SW 0 0% 0% [spi1]
359 2 root SWN 0 0% 0% [jffs2_gcd_mtd3]
Switch#
```

show file

Command

```
show file
```

Mode
Privilege mode

Parameters
None

Description
The show file command is used to display system files.

Examples

```
Switch#show file
size          date       time       name
--------       ------     ------    --------
724    Jan-01-1970  06:05:35  switch.cfg
9198805    Jan-01-1970  00:05:06  switch.tar.gz
Switch#
```

CPU protection command

cpu-protect enable

Command

```
cpu-protect enable
no cpu-protect enable
```

Mode

Global configuration mode

Parameters

None

Description

The cpu-protect enable command is to turn on CPU protection.
The no cpu-protect enable command is to disable CPU protection.

Examples

```
Turn on CPU protection
switch#con t
switch(config)#cpu-protect enable
switch(config)#
```

cpu-protect cos

Command

```
cpu-protect cos<cos-value> pps <pps-value>
```

Mode

Global configuration mode

Parameters

cos-value: range: <0-7>.
pps-value: range: <50-500>.

Description

Set the number of CPU packets per second on different pairs of columns.

Examples

Configure the number of CPUs on column 0 to 400 per second.

```
switch(config)#cpu-protect cos 0 pps 400
switch(config)#
```

show cpu-protect

Command

```
show cpu-protect
```

Mode

Privilege mode

Parameters

None

Description

The show cpu-protect command is used to display CPU protection information.

Examples

```
Switch#show cpu-protect
CPU Protect : ON
Total Receive Packets : 0
```

```
Total Discard Packets : 0
COS [Type]    PPS [Default]  Receive Packets  Discard Packets
------------  -------------  ---------------  ---------------
0 [FORWARD ]  200 [200]      0                0
1 [ICMP    ]  150 [150]      0                0
2 [LOCAL   ]  500 [500]      0                0
3 [MANAGE  ]  250 [250]      0                0
4 [ARP     ]  100 [100]      0                0
5 [PROTO   ]  500 [500]      0                0
6 [IPV6    ]  500 [500]      0                0
7 [NOT USED]  100 [100]      0                0
switch#
```

CHAPTER 02

PortCommands

Port General Configuration

interface

Command

```
interface <if-name-start> [if-name-end]
```

Mode

Global Configuration Mode/Interface Configuration Mode

Parameters

if-name-start: The name of the interface. For Layer 2 interfaces, 100-gigabit ports are prefixed with fe, gigabit ports are prefixed with ge, and 10-gigabit ports are prefixed with xe, followed by the module number/port number; Layer 3 interface names are prefixed with vlan, followed by the vlan id number; trunk interface names.
if-name-end: Layer 2 interface name, if present this parameter must be the same type and module as if-name-start:.

Description

The interfaceCommand is used to enter the configuration mode of one or a range of ports.

Examples

```
#Go to port ge1/1:
Switch(config)#interface ge1/1
#Enter port ge1/1-ge1/2:
Switch(config)#interface ge1/1 ge1/2
```

into aggregation port 1.

```
Switch(config)#interface trunk1
```

description

Command

```
description <line>
no description
```

Mode

Interface configuration mode.

Parameters

line: port description string.

Description

The descriptionCommand sets the port description, which can describe the port.
The no descriptionCommand cancels the configuration of the port description.

Examples

Set the description of port ge1/1 to: bulid 1 floor 5

```
Switch(config-ge1/1)#description bulid 1 floor 5
```

show interface

Command

```
show interface [<if-name>| statistics <if-name>]
```

Mode
Normal mode / Privilege mode

Parameters
if-name: Interface name.
statistics: Displays port incoming and outgoing packet statistics.

Description
The show interfaceCommand displays information about all Layer 2 and Layer 3 interfaces without parameters. Specify the interface name to display information about the specified Layer 2 or Layer 3 interface. show interface statistics Displays packet statistics for the specified interface.

Examples
Display information about the vlan1 interface.

```
Switch#show interface vlan1
Interface vlan1
Hardware Type: VLAN
MAC Address: 0000.0009.ac23
Flags: <UP,BROADCAST,RUNNING,MULTICAST>
Admin Status: UP
Operate Status: UP
Index: 2
Metric: 1
MTU: 1500
IP Address: 192.168.0.1/24
```

shutdown

Command

```
shutdown
no shutdown
```

Mode
Interface configuration mode

Parameters
None

Description
shutdown shuts down the port, and the administrative status of the port is DOWN.
no shutdown opens the port and the port's administrative status is UP.

Examples

```
#close port ge1/1:
Switch(config-ge1/1)#shutdown
Switch(config-ge1/1)#
```

speed

Command

```
Speed {autonegtiate | full-10 | full-100 | full-1000 | half-10 | half-100}
```

Mode
Interface configuration mode

Parameters
Autonegtiate: The rate duplex state is adaptive.
full-10: The rate duplex state is 10M full duplex.
full-100: The rate duplex state is 100M full duplex.
full-1000: The rate duplex state is 1000M full duplex.
half-10: The duplex state is 10M half-duplex.

half-100: The duplex state is 100M half-duplex.

Description
Sets the rate duplex state of the port.

Examples
Configure the rate duplex state of port ge1/1 to force 100M full duplex.
```
switch(config-ge1/1)#speed full-100
```

MIRRORCommand

mirror

Command
```
mirror interface <if-name>direction {both | receive | transmit}
no mirror interface <if-name> direction [receive | transmit]
```

Mode
Interface configuration mode.

Parameters
if-name: The port to be listened to.
both: Listen for incoming and outgoing data streams on the specified port.
receive: Listen for data streams received by the specified port.
transmit: Listens to the data stream output from the specified port.

Description
The mirror interfaceCommand specifies the port to be listened to, and is used to listen for data streams from other ports.
The no mirror interfaceCommand cancels the listening setting of the port.

Examples
```
#Listen to the incoming data stream on port ge1/2 with port ge1/1.
Switch(config-ge1/1)#mirror interface ge1/2 direction receive
Switch(config-ge1/1)#
```

show mirror

Command
```
show mirror [interface <if-name>]
```

Mode
Privilege mode

Parameters
interface <if-name>: Port name.

Description
The show mirrorCommand is used to display the mirror configuration of the specified port.

Examples
```
None.
```

Broadcast storm controlCommands

storm-control

Command
```
storm-control {broadcast | dlf | multicast}
no storm-control {broadcast | dlf | multicast}
```

Mode
Interface configuration mode

Parameters
broadcast: Control broadcast packets.
dlf: unicast packet with unknown control destination.
multicast: Control multicast packets.

Description
The storm-controlCommand is used to set the port's forwarding limit for broadcast packets, dlf packets, and multicast packets.
The no storm-controlCommand is used to cancel the setting.

Examples
```
Turn on the radio storm
Switch(config-ge1/1)#storm-control broadcast
```

storm-controlratelimit

Command
```
storm-control ratelimit<1-1024000>kbits
```

Mode
Interface configuration mode

Parameters
Level: control the forwarding rate, minimum limit value is 64 Kbits, granularity is also 64 Kbits.

Examples
```
Limit the forwarding speed of port ge1/1 to 1024 kbit/s for broadcast streams:
Switch(config-ge1/1)#storm-control ratelimit1024
```

show storm-control

Command
```
show storm-control [<if-name>]
```

Mode
Privilege mode

Parameters
if-name: The name of the port.

Description
The show storm-controlCommand is used to display the settings of storm-control, including the control values of broadcast packets, dlf packets, multicast packets and the number of dropped packets.

Examples
Displaying the storm-control configuration for port ge1/1.
```
Switch#sh storm-control ge1/1
Port Bcast Mcast Dlf Limit(kbits)
ge1/1 set unset unset 64
```

STORM-CONSTRAIN

storm-constrain

Command
```
storm-constrain {broadcast|multicast|unicast } min-rate <min-value> max-rate <max-value>
no storm-constrain { broadcast|multicast|unicast|all }
```

Mode
Interface configuration mode

Parameters
broadcast: Broadcast.
multicast: Multicast.
unicast: unicast.
min-value: minimum speed, the value range <1-1488100>
max-value: the maximum speed, the value range is <1-1488100>.

Description
The storm-constrainCommand is used to perform storm control on broadcast, multicast, or unknown unicast messages under the interface.
The no storm-constrainCommand cancels storm control

Examples
```
None.
```

storm-constrain action

Command
```
storm-constrain action {block|shutdown}
no storm-constrain action
```

Mode
Interface configuration mode

Parameters
Block: Blocking port.
Shutdown: Shut down the port.

Description
The storm-constrain actionCommand is used to configure the action of storm control. By default, no storm control is performed on the messages
The no storm-constrain actionCommand cancels the configured storm control action

Examples
```
None.
```

storm-constrain enable

Command
```
storm-constrain enable <log>
no storm-constrain enable <log>
```

Mode
Interface configuration mode

Parameters
Log: Log switch.

Description
The storm-constrain enableCommand is used to turn on the switch for logging during storm control
The no storm-constrain enableCommand disables the switch for logging during storm control

Examples
```
None.
```

storm-constraininterval

Command

```
storm-constrain interval <time-value>
no storm-constrain interval
```

Mode

Interface configuration mode

Parameters

time-value: the time interval value, in the range <6-180>.

Description

The storm-constrain intervalCommand is used to configure the detection interval of storm control, by default, the detection interval of storm control is 5 seconds

The no storm-constrain intervalCommand restores the detection interval for storm control to the default

Examples

```
None.
```

show storm-constrain

Command

```
show storm-constrain[interface <if-name>]
```

Mode

Privilege mode

Parameters

If-name:specific interface

Description

The show storm-constrainCommand is used to view the storm control information of all interfaces

The show storm-constrain interface <if-name>Command is used to view the storm control information of an interface

Examples

```
None.
```

FLOW-CONTROLCommand

flowcontrol

Command

```
flowcontrol
```

Mode

Interface configuration mode

Parameters

None

Description

The flowcontrolCommand is used to turn on or off the flow control function of the port, and can control whether to send flow control frames or whether to process the received flow control frames.

Examples

```
None.
```

show flowcontrol

Command

```
show flowcontrol [interface <if-name>]
```

Mode

Normal mode / Privilege mode

Parameters

if-name: The name of the interface.

Description

View the configuration of port flow control.

Examples

```
None.
```

Port speed limitCommand

portrate

Command

```
portrate egress <rate>
portrate ingress <rate>
```

Mode

Interface configuration mode.

Parameters

egress: port output rate.
ingress: port input rate.
rate: the set rate value, range: 1-1024000 kbits.

Description

Sets the maximum input and output rate of the port. The minimum limit is 64 Kbits, and the granularity is also 64 Kbits.

Examples

Set port ge1/1 input speed limit 128Kbps.

```
Switch(config-ge1/1)#portrate ingress 128
Switch(config-ge1/1)#
```

show portrate

Command

```
show portrate <if-name>
```

Mode

Privilege mode

Parameters

if-name: The name of the port.

Description

The show portrateCommand is used to display the speed limit configuration of the specified port.

Examples

```
None.
```

Port Link AggregationCommand

lacp system-priority

Command

```
lacp system-priority <pri-value>
no lacp system-priority
```

Mode

Global configuration mode

Parameters

pri-value: system priority, range <1-65535>

Description

lacp system-priority Sets the system priority.
no lacp system-priority restores the system priority default value of 32768.

Examples

```
Switch(config)#lacp system-priority 1
```

lacp max-active-link-number

Command

```
lacp max-active-link-number <num-value>
no lacp max-active-link-number
```

Mode

Global configuration mode

Parameters

num-value: activates aggregation range <1-8>

Description

lacp max-active-link-number Sets the maximum number of lacp active aggregation ports.
no lacp max-active-link-number Restores the lacp active aggregation port default limit of 8.

Examples

```
Switch(config)# lacp max-active-link-number 1
```

lacp port-priority

Command

```
lacp port-priority <pri-value>
no lacp port-priority
```

Mode

Interface configuration mode

Parameters

pri-value: interface priority, range <1-65535>

Description

lacp port-priority Sets the interface priority.
no lacp port-priority restores the default value of 32768 to the system interface prior level.

Examples

```
Switch(config-ge1/1)#lacp port-priority 1
```

lacp timeout

Command

```
lacp timeout { short|long }
```

Mode

Interface configuration mode

Parameters

None

Description

lacp timeout {short|long} Set the lacp port timeout, the default is long timeout.

Examples

```
None
```

show lacp summary

Command

```
show lacp summary
```

Mode

Privilege mode

Parameters

None.

Description

Displays a brief overview of all lacp aggregations.

Examples

```
None
```

show lacp detail

Command

```
show lacp detail
```

Mode

Privilege mode

Parameters

None.

Description

Displays all lacp aggregations.

Examples

```
None
```

show lacp

Command

```
show lacp <num-value>
```

Mode

Privilege mode

Parameters

num-value: lacp group number, value range <1-8>

Description

Displays the details of the lacp aggregation group.

Examples

None

show lacp port

Command

```
show lacp port <ifname>
```

Mode

Privilege mode

Parameters

ifname: specific interface

Description

Displays the details of the lacp port.

show lacp system-id

Command

```
show lacp system-id
```

Mode

Privilege mode

Parameters

None

Description

Displays the lacp system status.

show lacp counter

Command

```
show lacp counter [<num>]
```

Mode

Privilege mode

Parameters

num: lacp group number, in the range <1-8>

Description

Displays the statistics of the lacp aggregation port.
Displays the statistics of all lacp aggregation ports.

clear lacp

Command

```
clear lacp [<num>] counters
```

Mode

Privilege mode

Parameters

num: lacp group number, in the range <1-8>.

Description

Clear the statistics of lacp aggregation groups.
Clear the statistics of all lacp aggregation groups.

trunk

Command

```
trunk <trunk-id> [dynamic]
no trunk <trunk-id>
```

Mode

Global configuration mode.

Parameters

trunk-id: Link aggregation number, range <1-8>. No link aggregation is configured by default.

Description

The trunkCommand is used to create a link aggregation, and the system treats a link aggregation as a logical port. You need to create a link aggregation before you can configure the aggregated ports. Each trunk group supports up to 8 ports. no trunkCommand is used to delete a link aggregation. Before deleting a trunk group, you need to delete the member ports first.

Examples

Configure an aggregated link with group number 1.

```
Switch(config)#trunk ?
<1-8> Trunk id
Switch(config)#trunk 1
Switch(config)#
```

trunk interface

Command

```
trunk interface <if-name> [passive]
no trunk interface [<if-name>]
```

Mode

Interface configuration mode.

Parameters

if-name: The name of the port.

Description

The trunk interface <if-name>Command adds the physical port to the trunk group and becomes an aggregated port.

The no trunk interfaceCommand removes the physical port from the trunk group; if you enter a port name, only the specified port is removed; if you do not enter a port name, all physical ports in the trunk group are removed.

Examples

Configure port ge1/1 to become a member port of trunk1.

```
Switch(config-trunk1)#trunk interfae ge1/1
```

trunk load-balance

Command

```
trunk load-balance {dst-ip | dst-mac | src-dst-ip |src-dst-mac | src-ip |src-mac}
no trunk load-balance
```

Mode

Interface configuration mode.

Parameters

dst-ip: Load balancing the data flow in the outgoing port direction based on the destination IP address.
dst-mac: Load balancing the data flow in the outgoing port direction based on the destination MAC address.
src-dst-ip: Load balancing the data flow in the outgoing port direction based on the source and destination IP addresses.

src-dst-mac: The data flow in the outgoing port direction based on the source MAC address and the destination MAC address
Load Balancing. This is the default load balancing policy.
src-ip: Load balancing the data flow in the outgoing port direction based on the source IP address.
src-mac: Load balancing the data flow in the outgoing port direction based on the source MAC address.

Description
The trunk load-balanceCommand sets the load balancing policy of the TRUNK group.
The no trunk load-balanceCommand cancels the configured load balancing policy and reverts to the src-dst-mac policy.

Examples
Configure trunk group 1 to load balance based on the destination IP address.

```
Switch(config-trunk1)#trunk load-balance dst-ip
```

show trunk

Command

```
show trunk [<trunk-id>]
```

Mode
Privilege mode.

Parameters
trunk-id: ID number of the TRUNK group to be queried.

Description
Displays the link aggregation configuration, including trunk group name, load balancing policy, and member ports. If you do not specify the trunk group ID number, all the aggregation port configurations are displayed.

Examples
Show all link aggregation configurations.

```
Switch#show trunk
% Trunk name: trunk15
% Load-balance: Source and Destination Mac address
% Member:
ge1/6
ge1/10
% Trunk name: trunk10
% Load-balance: Source and Destination Mac address
% Member:
ge1/11
ge1/12
Switch#
```

debug lacp

Command

```
[no] debug lacp [all | cli |event | packets | sync | timer]
```

Mode
Privilege mode

Parameters
None.

Description
The debug lacpCommand is used to turn on the debug switch related to the lacp protocol and write the related logs to the log table

Examples

```
None
```

Oversize frameCommand

jumbo frame

Command

```
jumbo frame<1523-16318>
no jumbo frame
```

Mode

Interface configuration mode

Parameters

1523: Allow packets of 1523 bytes in length to pass
16318: allows packets of 16318 bytes in length to pass

Description

The jumbo frameCommand configures the length of globally forwardable packets.
The no jumbo frameCommand reverts to the default value of 1522 bytes.

Examples

Configure the port to forward packets up to 2044 bytes in length

```
Switch(config-ge1/1)#jumbo frame 1523
```

show jumbo frame

Command

```
show jumbo frame [if-name]
```

Mode

Normal mode / Privilege mode

Parameters

if-name: interface number

Description

show jumbo frame to view mega frame configuration

Examples

Show jumbo frame configuration.

```
Switch#show jumbo frame ge1/1
Port Jumbo frame(bytes)
```

Redundant PortCommands

redundant-port

Command

```
redundant-port <redundant-id> primary-port <if-name> secondary-port <if-name> [force-Switch]
no redundant-port < redundant-id >
```

Mode

Global configuration mode.

Parameters

redundant-id: Redundant port group, range <1-8>.
if-name: The name of the port.
force-Switch : Whether to enable the force switch.

Description

redundant-port <redundant-id> Configures a set of redundant ports, configuring the primary port and and standby port as a set to make them redundant.
The no redundant-port <redundant-id>Command is to remove the redundant port

Examples
Configure redundant port group 1, ge1/1 is the primary port, ge1/2 is the standby port without forced switchover enabled.

```
Switch(config)#redundant-port 1 primary-port ge1/1 secondary-port ge1/2
```

redundant-port force-Switch

Command

```
redundant-port < redundant-id > force-Switch
no redundant-port < redundant-id > force-Switch
```

Mode
Global configuration mode.

Parameters
redundant-id: Redundant port group, range <1-8>.

Description
The redundant-port < redundant-id > force-SwitchCommand enables the force switch for redundant ports.
The no redundant-port < redundant-id > force-SwitchCommand disables the force switch for redundant ports.

Examples
Enable redundant port group 1 forced toggle switch.

```
Switch(config)#redundant-port 1force-Switch
```

show redundant-port

Command

```
show redundant-port
```

Mode
Normal mode / Privilege mode.

Parameters
None.

Description
Displays the redundant port configuration, including the redundant port group ID, the primary port, the standby port, and the status of the port.

Examples
Display redundant port group information.

```
Switch#show redundant-port
Group <1> Force-Switch <Enable>
primary-port <ge1/1> state <Active>
secondary-port <ge1/2> state <Disabled>
```

UDLDCommands

udld enable

Command

```
udld enable
no udld enable
```

Mode
Global configuration mode

Parameters
None.

Description
The udld enableCommand is used to globally enable the udld function
The no udld enableCommand is used to globally disable the udld function

Examples
```
switch(config)# udld enable
switch(config)# no udld enable
```

udld message time

Command
```
udld message time<time>
no udld message time
```

Mode
Global configuration mode

Parameters
time: udld message delivery interval, in the range <7-19>

Description
The udld message timeCommand is used to set the interval for sending udld messages.
The no udld message timeCommand is used to restore the udld message delivery interval.

Examples
```
Switch(config)#udld message time 7
```

udld port

Command
```
udld port
no udldport
```

Mode
Interface configuration mode

Parameters
None.

Description
The udld portCommand is used to enable the port udld
The no udldportCommand is used to shut down the port udld

Examples
```
Switch(config-ge1/1)#udld port
Switch(config-ge1/1)#noudld port
```

udld aggressive

Command
```
[no] udld aggressive
```

Mode
Interface configuration mode

Parameters
None.

Description
The udld aggressiveCommand is used to enable port aggressive mode

The no udld aggressiveCommand is used to restore the port to normal mode, the default normal mode

Examples

```
Switch(config-ge1/1)#udld aggressive
Switch(config-ge1/1)#no udld aggressive
```

show udld

Command

```
show udld[if-name]
```

Mode

Privilege mode

Parameters

if-name: Port number.

Description

The show udldCommand is used to view port udld information

Examples

```
Switch#show udld
Interface ge1/1:
---
Global enable state: Enabled
Port enable state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

debug udld

Command

```
[no] debug udld[all |events]
```

Mode

Privilege mode

Parameters

None.

Description

The debug udldCommand is used to turn on the debug switch of the udld protocol and write the relevant logs to the log table

Examples

```
Switch#debug udld all
Switch#
```

debug udld packet

Command

```
[no] debug udld packets [ recv |send]
```

Mode

Privilege mode

Parameters

None.

Description
The debug udldpacketsCommand is used to turn on the debug switch for udld protocol messages and write the relevant logs to the log table

Examples
```
Switch#debug udld packets recv
```

LLDPCommands

lldp global enable

Command
```
lldp global enable
no lldp global enable
```

Mode
Global configuration mode.

Parameters
None.

Description
The lldp global enable global enable lldpCommand.
The no lldp global enableCommand is used to disable lldp

Examples
```
Switch(config)#lldp global enable
Switch(config)#no lldp global enable
```

lldp hold-multiplier

Command
```
lldp hold-multiplier<number>
no lldp hold-multiplier
```

Mode
Global configuration mode.

Parameters
Number: ttl multiplier, range 2-10

Description
The lldp hold-multiplierCommand sets the lldp ttl multiplier.
The no lldp hold-multiplierCommand is used to remove the lldp ttl configuration and restore the default value.

Examples
```
Switch(config)#lldp hold-multiplier 2
Switch(config)#no lldp hold-multiplier
```

lldp timer

Command
```
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]
no lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]
```

Mode
Global configuration mode.

Parameters
reinit-delay<time>: specific time, in the range 1-10.
tx-delay<time>: specific time, in the range 1-10.
tx-interval <time>: specific time, in the range 5-300.

Description
The lldp timerCommand sets various timers for lldp.
The no lldp timerCommand is used to remove the lldp various timer configurations and restore the default values.

Examples

```
Switch(config)#lldp timer reinit-delay 1
Switch(config)#lldp timer tx-delay 1
Switch(config)#lldp timer tx-interval 5
Switch(config)#no lldp timer reinit-delay
Switch(config)#no lldp timer tx-delay
Switch(config)#no lldp timer tx-interval
```

lldp enable

Command

```
lldp enable
no lldp enable
```

Mode
Interface configuration mode.

Parameters
None.

Description
The lldp enableCommand enables the interface lldp
The no lldp enableCommand disables the interface lldp

Examples

```
Switch(config-ge1/1)#lldp enable
Switch(config-ge1/1)#no lldp enable
```

lldp admin-status

Command

```
lldp admin-status{disable | rx | tx| rxtx}
```

Mode
Interface configuration mode.

Parameters
None.

Description
The lldp admin-statusCommand configures the lldp port operating mode

Examples

```
Switch(config-ge1/1)#lldp admin-status rx
```

lldp check-change-interval

Command

```
lldp check-change-interval<time>
no lldp check-change-interval
```

Mode
Interface configuration mode.

Parameters
time:refresh time interval of interface information, range 1-30

Description
The lldp check-change-intervalCommand is used to configure the time interval for refreshing interface information
The no lldp check-change-intervalCommand restores the default time interval for refreshing interface information

Examples
```
Switch(config-ge1/1)#lldp check-change-interval 1
Switch(config-ge1/1)#no lldp check-change-interval
```

lldp management-address

Command
```
lldp management-address<if-name>
no lldp management-address
```

Mode
Interface configuration mode.

Parameters
if-name:ip address.

Description
The lldp management-addressCommand is used to configure the interface lldp management address
The no lldp management-addressCommand removes the interface management address

Examples
```
Switch(config-ge1/1)#lldpmanagement-address1.1.1.1
Switch(config-ge1/1)#no lldp management-address
```

lldp tlv-enable

Command
```
[no] lldp tlv-enable{dot1-tlv| dot3-tlv|med-tlv }
```

Mode
Interface configuration mode.

Parameters
None.

Description
The lldp tlv-enableCommand is used to configure the interface lldp extended capability set switch
The no lldp tlv-enableCommand removes the interface lldp extended capability switch

Examples
```
Switch(config-ge1/1)#lldp tlv-enable dot1-tlv
Switch(config-ge1/1)#no lldp tlv-enable dot1-tlv
```

show lldp configuration

Command
```
show lldp configuration [if-name]
```

Mode
Privilege mode.

Parameters
if-name: Interface number.

Description
The show lldp configurationCommand is used to display lldp configuration information

Examples

```
Switch#show lldp configuration ge1/1
LLDP global status: Enable
LLDP tx interval: 5
LLDP tx hold: 2
LLDP tx delay: 1
LLDP reinit delay: 1
Port ge1/1 Configuration:
LLDP status: Enable
Admin status: enabledRxOnly
Check local change: Disable
Management address: 1.1.1.1
Dot1-tlv: Disable
Dot3-tlv: Enable
Med-tlv: Enable
```

show lldp local-information

Command

```
show lldp local-information [if-name]
```

Mode

Privilege mode.

Parameters

if-name: Interface number.

Description

The show lldp local-informationCommand is used to display lldp local information

Examples

```
Switch#sh lldp local-information ge1/1
```

show lldp neighbor-information

Command

```
show lldp neighbor-information [if-name]
```

Mode

Privilege mode.

Parameters

if-name: Interface number.

Description

The show lldp neighbor-informationCommand is used to display lldp neighbor information

Examples

```
None.
```

show lldp lldp statistics

Command

```
show lldp statistics [if-name]
```

Mode

Privilege mode.

Parameters

if-name: Interface number.

Description

The show lldp statisticsCommand is used to display lldp message statistics

Examples

```
Switch#sh lldp statistics
PortLocal ge1/1:
statsFramesOutTotal: 0
statsAgeoutsTotal: 0
statsFramesDiscardedTotal: 0
statsFramesInErrorsTotal: 0
statsFramesInTotal: 0
statsTLVsDiscardedTotal: 0
statsTLVsUnrecognizedTotal: 0
```

show lldp status

Command

```
show lldp status [if-name]
```

Mode

Privilege mode.

Parameters

if-name: Interface number.

Description

The show lldp n statusCommand is used to display lldp status information

Examples

```
Switch#sh lldp status
PortLocal ge1/1:
LLDP status: Enable
adminStatus: enabledRxOnly
portEnabled: FALSE
tx state: TX_LLDP_INITIALIZE
somethingChangedLocal:: FALSE
txTTL: 10
msgTxInterval: 5
msgTxHold: 2
txDelay: 1
reinitDelay: 1
txTTR: 0
txDelayWhile: 0
txShutdownWhile: 0
rx state: LLDP_WAIT_PORT_OPERATIONAL
badFrame: FALSE
rcvFrame: FALSE
rxChanges: FALSE
rxInfoAge: FALSE
rxTTL: 0
somethingChangedRemote:: FALSE
tooManyNeighbors:: FALSE
tooManyNeighborsTimer: 0
```

debug lldp

Command

```
[no] debug lldp [all |events]
```

Mode

Privilege mode

Parameters
None.

Description
The debug lldpCommand is used to turn on the debug switch of the lldp protocol and write the relevant logs to the log table

Examples
```
Switch#debug lldp all
Switch#
```

debug lldp packet

Command
```
[no] debug lldp packets [ recv |send]
```

Mode
Privilege mode

Parameters
None.

Description
The debug lldp packetsCommand is used to turn on the debug switch of lldp protocol packets and write the relevant logs to the log table

Examples
```
Switch#debug lldp packets recv
Switch#
```

CHAPTER 03

Port-based security commands

MAC Binding Command

switchport port-security mac-bind

Command

```
switchport port-security mac-bind <mac-address> vlan <vlan-id> {qosprofile <qp-value> }
no switchport port-security mac-bind [mac-address]
```

Mode

Interface configuration mode.

Parameters

mac-address: the physical address of the binding, expressed in 12-bit hexadecimal; the mac address, in the format HHHH.HHHH.HHHH.
vlan-id: The id number of the vlan for mac-bind, in the range 1-4094.
qp-value: the pair of packets,the values are qp0,qp1,qp2,qp3,qp4,qp5,qp6,qp7.

Description

The switchport port-security mac-bind command applies mac binding to the port.
The no switchport port-security mac-bind command cancels the mac binding.

Examples

Configure port ge1/1 in vlan1 in for MAC binding 00ca.0009.0001.

```
Switch(config-ge1/1)#switchport port-security mac-bind 00ca.0009.0001 vlan 1
Switch(config-ge1/1)#
```

switchport port-security mac-bind auto-conversion

Command

```
switchport port-security mac-bind auto-conversion [number <number> [qosprofile < qp-value>] | vlan
<vlan-id> [qosprofile <qp-value> qp-value>] | qosprofile < qp-value>]
```

Mode

Interface configuration mode.

Parameters

number: the number of mac auto-binding, in the range of 1-1891.
vlan-id: the mac binding for which vlan, range 1-4094.
qp-value: the pair of packets,the values are qp0,qp1,qp2,qp3,qp4,qp5,qp6,qp7.

Description

The switchport port-security mac-bind auto-conversion command performs automatic binding of learned dynamic mac addresses.

Examples

Configure dynamic mac addresses learned under port ge1/1 to be automatically converted to static mac address bindings.

```
Switch(config-ge1/1)#switchport port-security mac-bind auto-conversion
Switch(config-ge1/1)#
```

show port-security mac-bind

Command

```
show port-security mac-bind [ifname]
```

Mode

Normal mode / Privilege mode

Parameters

ifname: The name of the Layer 2 interface to be specified.

Description

Displays information about the mac binding of the specified port.

Examples

```
Switch#show port-security mac-bind
VLAN ID MAC ADDRESS IFNAME
00ca.0009.0001 ge1/12
Switch#
```

MAC filtering commands

switchport port-security mac-filter

Command

```
switchport port-security mac-filter <mac-address> vlan <vlan-id>
no switchport port-security mac-filter [mac-address]
```

Mode

Interface configuration mode.

Parameters

mac-address: the physical address of the filter, expressed in 12-bit hexadecimal; the mac address, in the format HHHH.HHHHH.
vlan-id: The id number of the vlan for mac-bind, in the range 1-4094.

Description

The switchport port-security mac-filter command applies mac filtering to the port. After successful configuration, the MAC address can only communicate within the bound vlan.
The no switchport port-security mac-filter command cancels mac filtering.

Examples

Configure port ge1/1 in vlan1 in for MAC filtering 00ca.0009.0001.

```
Switch(config-ge1/1)#switchport port-security mac-filter 00ca.0009.0001 vlan 1
Switch(config-ge1/1)#
```

switchport port-security mac-filter auto-conversion

Command

```
switchport port-security mac-filter auto-conversion [number <number> | vlan <vlan-id> ]
```

Mode

Interface configuration mode.

Parameters

number: the number of mac auto-filtering, in the range of 1-8191.
vlan-id: Which vlan to mac filter on, range 1-4094.

Description

The switchport port-security mac-filter auto-conversion command automatically converts learned dynamic mac addresses into mac address filters.

Examples

Configure dynamic mac addresses learned under port ge1/1 to be converted to static mac address filtering.

```
Switch(config-ge1/1)#switchport port-security mac-filter auto-conversion
Switch(config-ge1/1)#
```

show port-security mac-filter

Command

```
show port-security mac-filter [ifname]
```

Mode

Normal mode / Privilege mode

Parameters

ifname: The name of the Layer 2 interface to be specified.

Description

Displays information about mac filtering for the specified port.

Examples

```
Switch#show port-security mac-filter
VLAN ID MAC ADDRESS IFNAME
1 0009.ca00.0009 ge1/2
Switch#
```

MAC address learning control commands

switchport port-security learn-limit

Command

```
switchport port-security learn-limit <number>
no switchport port-security learn-limit
```

Mode

Interface configuration mode.

Parameters

number: Limit the number of MACs to be learned, in the range of 0-1000.

Description

The switchport port-security learn-limit command places a limit on the number of MACs a port can learn.
The no switchport port-security learn-limit command cancels the learn-MAC limit.

Examples

Configure port ge1/1 to learn only 50 MAC addresses.

```
Switch(config-ge1/1)#switchport port-security learn-limit 50
Switch(config-ge1/1)#
```

show port-security learn-limit

Command

```
Switch#show port-security learn-limit [ifname]
```

Mode

Normal mode / Privilege mode

Parameters

ifname: The name of the Layer 2 interface to be specified.

Description

Displays the number of MACs learned on the specified port.

Examples

```
Switch#show port-security learn-limit
interface ge1/2 dynamic learn limit is 50.
Switch#
```

Protect port command

switchport port-security protect

Command

```
switchport port-security protect
no switchport port-security protect
```

Mode

Interface configuration mode.

Parameters

None.

Description

The switchport port-security protect command configures the port as a protected port.
The no switchport port-security protect command unprotects the port.

Examples

Configure port ge1/1 as a protected port

```
Switch(config-ge1/1)#switchport port-security protect
```

show port-security protect

Command

```
show port-security protect
```

Mode

Normal mode/privileged mode.

Parameters

None.

Description

Displays protected port information.

Examples

Show all protected port configurations.

```
Switch(config-ge1/1)#show port-security protect
Port Port protected
----- --------------
ge1/1 ON
Switch#
```

CHAPTER 04

ip mac-bind

ip mac-bind configuration command

ip mac-bind

Command

```
ip mac-bind <source-ip><mac-address>
no ip mac-bind <source-ip><mac-address>
```

Mode

Interface configuration mode.

Parameters

source-ip: source IP format A.B.C.D.
mac-address: mac address, format HHHH.HHHH.

Description

The ip mac-bind command is to bind the ip to the mac address under the port.

Examples

```
Switch(config-ge1/3)#ip mac-bind 192.168.0.2 0009.ca00.0002
```

ip mac-bind View command

show ip mac-bind

Command

```
show ip mac-bind [if-name]
```

Mode

Normal mode / Privilege mode.

Parameters

if-name: Interface name.

Description

The show ip mac-bind command views ip mac-bind information.

Examples

```
Switch#show ip mac-bind
[ge1/4] sum: 1
MAC IP
0009.ca00.0020 192.168.0.200
```

CHAPTER 05

Port Loop Detection

Port Loop Detection Configuration Commands

loop-detection detection-detection-time

Command

```
loop-detection detection-detection-time <time>
no loop-detection detection detection-time
```

Mode

Global configuration mode.

Parameters

time: Loop detection interval, range <1-65535> default is 5 seconds.

Description

The loop-detection detection-detection-time command configures the time period for loop detection. 2 times this time must be less than the recovery time period. the default value is 5 seconds.
The no loop-detection detection-time command restores the default loop detection time.

Examples

Set the default loop detection time to 6 seconds.

```
Switch#configure terminal
Switch(config)#loop-detection detection-detection-time 6
Switch#
```

loop-detection resume-mode

Command

```
loop-detection resume-mode {automation [<time>] | manual}
no loop-detection resume-mode
```

Mode

Interface configuration mode.

Parameters

time: auto recovery time, range <10-65535> default is 600 seconds.

Description

The loop-detection resume-mode command configures the recovery mode, choosing whether to recover manually or automatically, and the automatic recovery can also configure a recovery time, which is automatic by default.
The no loop-detection resume-mode command is to revert to automatic recovery.

Examples

Set the automatic recovery time to 60 seconds.

```
Switch#configure terminal
Switch(config)#loop-detection resume-mode automation 60
Switch#
```

loop-detection protocol-safety

Command

```
loop-detection protocol-safety
no loop-detection protocol-safety
```

Mode

Global configuration mode.

Parameters

None.

Description

The loop-detection protocol-safety command configures to enable protocol security checking, which is disabled by default.

The no loop-detection protocol-safety command disables protocol security checking.

Examples

Set to enable protocol security checks.

```
Switch#configure terminal
Switch(config)# loop-detection protocol-safety
Switch#
```

loop-detection respond-packets

Command

```
loop-detection respond-packets < number >
no loop-detection respond-packets
```

Mode

Global configuration mode.

Parameters

number: Configure the number of packets that must be received within a certain period of time. This configuration will take effect if protocol security checking is enabled, the default value is 10, in the range <2-100>.

Description

The loop-detection respond-packets command configures the number of packets that must be received when protocol security checking is enabled.

The no loop-detection respond-packets command restores the number of packets received to the default value when protocol security checking is enabled.

Examples

Set the number of packets that must be received when protocol security checks are enabled to 20.

```
Switch#configure terminal
Switch(config)# loop-detection respond-packets 20
Switch#
```

loop-detection resume-time

Command

```
loop-detection resume-time < time >
no loop-detection resume-time
```

Mode

Global configuration mode.

Parameters

time: auto recovery time, range <10-65535> default is 30 seconds.

Description

The loop-detection resume-time command configures the time period for automatic recovery, which must be greater than 2 being of the loop check time, and this configuration will take effect if automatic recovery is enabled. The default recovery time is 600 seconds.
The no loop-detection resume-time command restores the auto-resume time to its default value.

Examples

Set the automatic recovery time to 20,.

```
Switch#configure terminal
Switch(config)# loop-detection resume-time 20
Switch#
```

loop-detection enable

Command

```
loop-detection enable
no Loop-detection enable
```

Mode

Interface configuration mode.

Parameters

None.

Description

The Loop-detection enable command turns on the port loop detection function.
The no Loop-detection enable command is to disable the port loop detection function.

Examples

Set port ge1/1 to start loop detection,.

```
Switch#configure terminal
Switch(config)#int ge1/1
Switch(config-ge1/1)#loopback-detection enable
Switch#
```

loop-detection resume

Command

```
loop-detection resume
```

Mode

Interface configuration mode.

Parameters

None.

Description

The Loop-detection resume command manually resumes and restarts the loop check.

Examples

Set port ge1/1 to manually restore and restart loop checking with.

```
Switch#configure terminal
Switch(config)#int ge1/1
Switch(config-ge1/1)#loopback-detection resume
Switch#
```

loopback-detection shutdown-mode

Command

```
loopback-detection shutdown-mode {no-shutdown | shutdown}
```

Mode
Interface configuration mode.

Parameters
None.

Description
The loopback-detection shutdown-mode command configures whether the port shuts down when a loopback occurs.

Examples
Set the port to shutdown when a loop occurs on port ge1./1.

```
Switch#configure terminal
Switch (config)#interface ge1/1
Switch(config-ge1/1)#loopback-detection shutdown-mode shutdown
Switch#
```

Port Loop Detection View Command

show loop-detection

Command

```
Show loop-detection [ifname]
```

Mode
Normal mode / Privilege mode

Parameters
Ifname: The name of the interface.

Description
The show loop-detection command is to display all configurations of a protocol and the configuration of an interface.

Examples
Show port loop detection configuration:

```
Switch#show loop-detection
Loop detection configuration information
detection interval : [5 Secs.] Default[5 Secs.]
Resume mode : [Automation] Default[Automation]
Resume interval : [600 Secs.] Default[600 Secs.]
Execute operate : [Shutdown] Default[Shutdown]
Protocol safety : [Disable] Default[Disable]
Respond packets : [10] Default[10]
PortDected List :
Switch#
```

Port Loop Detection Debug Command

debug loop-detection

Command

```
[no] debug loop-detection [all | events]
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description

debug loop-detection is used to turn on the debug switch related to the loop-detection protocol and write the related logs to the log table.

Examples

```
#No
```

debug loop-detectionpackets

Command

```
[no] debug loop-detectionpackets [recv | send]
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

debug loop-detection packets is used to turn on the debug switch related to loop-detection packets and write the related logs to the log table.

Examples

```
#No
Switch#debug loop-detection packets recv
Switch#show debugging loo
Switch# show debugging loop-detection
loopback-detection debugging status:
loopback-detection packets receive debugging is on
Switch#
```

CHAPTER 06

Vlan commands

vlan creation command

vlan database

Command

```
vlan database
```

Mode

Global configuration mode

Parameters

None.

Description

Enter vlan configuration mode.

Examples

Enter vlan configuration mode.

```
Switch(config)#vlan database
Switch(config-vlan)#
```

vlan

Command

```
vlan <vlan-id>
no vlan <vlan-id>
```

Mode

vlan configuration mode

Parameters

vlan-id: The vlan number to be created. The input method can be 2,4,6 or 3-10, the range of values: 2~4094

Description

The vlan command is used to create a VLAN. it should be noted that VLAN 1 is the default VLAN and cannot be deleted.

The no vlan command is used to delete a vlan or a group of vlan.

Examples

```
#Create vlan 2.
Switch(config-vlan)#vlan 2
Switch(config-vlan)#
```

vlan port configuration commands

switchport access

Command

```
switchport access vlan <vlan-id>
no switchport access vlan
```

Mode

Interface configuration mode

Parameters
vlan-id: The default VID of the port, in the range 2-4094.
There is only VLAN 1 in the default switch, and all ports are untagged members of VLAN 1.

Description
The switchport access command is used to set a Layer 2 interface whose VLAN mode is ACCESS to the specified VLAN. this command is valid only for Layer 2 interfaces whose VLAN mode is ACCESS mode. After setting this command, the PVID of this Layer 2 interface is the specified VLAN, and this Layer 2 interface belongs to the UNTAG member of the specified VLAN only.
The no switchport access vlan command returns the interface's access vlan to the default VLAN, VLAN 1. After this command is set, the pvid of this interface changes to 1 and belongs to the untagged members of VLAN 1 only.

Examples
Configure port ge1/1 as untagged port for vlan2.

```
Switch(config-ge1/1)#switchport access vlan 2
```

switchport hybrid allowed vlan add

Command

```
switchport hybrid allowed vlan add<vlan-list>egress-tagged { disable | enable}
```

Mode
Interface configuration mode

Parameters
vlan-list: vlan number of the joined vlan, range 1-4094.

Description
The switchport hybrid command is used to add the port to the specified VLAN or VLANs. If it is egress-tagged enable, it is a TAG member, and if it is egress-tagged disable, it is a UNTAG member.
There are two ways to express <vlan_list>, one is multiple VLAN numbers separated by commas, such as 1,3,5,10, and the other is a VLAN range, such as 2-10, but both cannot exist at the same time.
Expressions 1,3-5 are wrong (, and - can exist only one), 2-4, 6-7 are also wrong (- can exist only once).

Examples
Set port ge1/1 as tagged port for vlan1-3.

```
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan add 1-3 egress-tagged enable
Switch(config-ge1/1)#
```

switchport hybrid allowed vlan all

Command

```
switchport hybrid allowed vlan all
```

Mode
Interface configuration mode

Parameters
None

Description
The switchport hybrid allowed vlan all command is valid only for Layer 2 interfaces in hybrid mode. The interface is added to all VLANs (except VLAN1) and is a tagged member of all VLANs. When a new VLAN is created in the future, the port will also be added to the new VLAN and is a TAGged member of that VLAN. After executing this command, the original UNTAG member of the port belongs to the active vlan will become a TAG member.

Examples
Set port ge1/1 as untagged member of vlan1 and tagged member of all other vlan:

```
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan all
```

switchport hybrid allowed vlan none

Command

```
switchport hybrid allowed vlan none
```

Mode

Interface configuration mode

Parameters

None

Description

This command is valid only for hybrid mode Layer 2 interfaces. The interface is no longer a member of all VLANs (except VLAN1). After executing this command, the native vlan of the port will be restored to 1.

Examples

port ge1/1 was originally tagged port for vlan1, untagged port for vlan2, vlan3, vid=2; remove ge1/1 from vlan outside of vlan1:

```
Switch(config-ge1/1)#switchport hybrid allowed vlan none
After executing this command, port ge1/1 is the tagged port of vlan1 with vid=1.
```

switchport hybrid allowed vlan remove

Command

```
switchport hybrid allowed vlan remove <vlan-id>
```

Mode

Interface configuration mode

Parameters

vlan-id: The vlan number to be removed, range 1-4094.

Description

This command is valid only for hybrids mode Layer 2 interfaces. The interface is no longer a member of one or more of the specified VLANs.
If there is an active vlan in the specified VLAN, the native vlan reverts to 1.

Examples

```
#Remove port ge1/1 from vlan2.
Switch(config-ge1/1)#switchport hybrid allowed vlan remove 2
```

switchport hybrid native vlan

Command

```
switchport hybrid native vlan <vlan-id>
no switchport hybrid native vlan
```

Mode

Interface configuration mode

Parameters

vlan-id: The vlan number of the joined vlan.

Description

This command is valid only for the layer 2 interface in hybrid mode. After setting this command, the pvid of this Layer 2 interface is the specified VLAN, and the interface belongs to the untagged member of the specified VLAN (if the port already belongs to the TAG member of the VLAN before setting this command, the port will continue to be the TAG member after executing this command). (If the port is already a TAG member of the VLAN before setting this command, the port will remain a TAG member after executing this command, and the PVID will still be the specified VLAN).

The no switchport hybrid vlan command restores the native vlan of the interface to the default VLAN (VLAN1). After executing this command, the original native vlan is deleted (no longer a UNTAG or TAG member of the original native vlan) and the new native vlan is 1, which is a UNTAG member of VLAN1 (if the port was already a TAG member of VLAN1 before executing this command, it will remain a TAG member of VLAN1 after executing this command), and the PVID is modified to 1. (if the port was already a TAG member of VLAN1 before executing this command, it will continue to be a TAG member of VLAN1 after executing this command) and the PVID is modified to 1.

Examples

Configure port ge1/1 as an untagged member of vlan2, a tagged member of vlan1, and with vid 2.

```
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#swi hybrid native vlan 2
Switch(config-ge1/1)#switchport hybrid allowed vlan add 1 egress-tagged enable
```

switchport mode

Command

```
switchport mode { access | hybrid | trunk}
no switchport { access | hybrid | trunk}
```

Mode

Interface configuration mode

Parameters

access: The interface vlan mode is access mode. The default is access mode. If the Layer 2 interface is set to ACCESS mode, the interface is by default a UNTAG member of VLAN1 with a PVID of 1.
hybrid: The interface vlan mode is hybrid mode. If the interface is set to HYBRID mode, the interface is by default a UNTAG member of VLAN1 with a PVID of 1.
trunk: The interface vlan mode is trunk mode. If the interface is set to TRUNK mode, the interface is by default a TAG member of VLAN1 with a PVID of 1.

Description

Set the VLAN mode of the Layer 2 interface, which is one of access, hybrid, or trunk.
The no switchport command restores the interface mode to the default value, returns to access mode, and the access vlan is VLAN1.

Examples

Set port ge1/1 as trunk port.

```
Switch(config-ge1/1)#switchport mode trunk
```

switchport trunk allowed vlan add

Command

```
switchport trunk allowed vlan add <vlan-list>
```

Mode

Interface configuration mode

Parameters

vlan-id: one or more VLAN numbers joined by this interface. the range of VLAN ID is 1-4094. there are two ways to express <vlan-id>, one is multiple VLAN numbers separated by commas, such as 1,3,5,10, and the other is a VLAN range, such as 2-10, but both ways cannot exist at the same time.

Description

This command is valid only for Layer 2 interfaces in trunk mode. The interface is joined to one or more specified VLANs and becomes a tagged member of the specified VLAN.

Examples

```
#Port ge1/1 is configured as a tagged member of vlan1-10.
Switch(config-ge1/1)#switchport trunk allowed vlan add 1-10
```

switchport trunk allowed vlan all

Command

```
switchport trunk allowed vlan all
```

Mode

Interface configuration mode

Parameters

None

Description

This command is valid only for Layer 2 interfaces in trunk mode. The interface is added to all VLANs (except VLAN1) and is a TAGGED member of all VLANs. When a new VLAN is created in the future, the port is also added to the new VLAN and is a TAGged member of that VLAN.

Examples

```
#Port ge1/1 is configured as a tagged member of all vlan's.
Switch(config-ge1/1)#switchport trunk allowed vlan all
```

switchport trunk allowed vlan none

Command

```
switchport trunk allowed vlan none
```

Mode

Interface configuration mode

Parameters

None

Description

This command is valid only for Layer 2 interfaces in trunk mode. The interface is no longer a member of any VLAN (except VLAN1).

Examples

remove trunk port ge1/1 from other vlan outside of vlan1.

```
Switch(config-ge1/1)#switchport trunk allowed vlan none
```

switchport trunk allowed vlan remove

Command

```
switchport trunk allowed vlan remove <vlan-list>
```

Mode

Interface configuration mode

Parameters

vlan-list: One or more VLAN numbers to be removed from this interface. the range of VLAN IDs is 1-4094. vlan-list has two expressions, one is multiple VLAN numbers separated by commas, such as 1,3,5,10, and the other is a VLAN range, such as 2-10, but both cannot exist at the same time.

Description

This command is valid only for Layer 2 interfaces in trunk mode. The interface is no longer a member of one or more of the specified VLANs.

Examples

```
#Remove port ge1/1 from vlan 2, vlan 3.
Switch(config-ge1/1)#switchport trunk allowed vlan remove 2,3
```

Switchport trunk native vlan

Command

```
Switchport trunk native vlan <vlan-id>
```

Mode

Interface configuration mode

Parameters

vlan-id: Default VLAN ID. the range of VLAN ID is 2-4094.

Description

This command is valid only for trunk mode Layer 2 interfaces. Set the default VLAN for this interface.

Examples

The default VLAN for port ge1/1 is VLAN2.

```
Switch(config-ge1/1)#Switchport trunk native vlan 2
```

vlan view command

show vlan

Command

```
show vlan [<vlan-id>]
```

Mode

Normal mode / Privilege mode

Parameters

vlan-id: The vlan number to be displayed, in the range of 1-4094.

Description

Displays information about the VLAN, including the information about the ports in the VLAN. When vlan id is specified, only the information of the specified vlan is displayed.

Examples

```
Switch#show vlan
VLAN Name State Member ports ([u]-Untagged, [t]-Tagged)
---- -------- --------- -------------------------------------------------
1 vlan1 active [u]ge1/1 [u]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
[u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
[u]ge1/11 [u]ge1/12
```

mac and ip subnet and protocol based vlan commands

mac-vlan

Command

```
mac-vlanmac <mac-address> vlan <vlan-id>
no mac-vlan [mac <mac-address>]
```

Mode

vlan configuration mode

Parameters

mac-address: mac address, format HHHH.HHHH.
vlan-id: The range of VLAN ID is 1-4094. vlan-id needs to be added first.

Description

The mac-vlanmac <mac-address> vlan <vlan-id> command is used to create a VLAN based on the source MAC address.
The no mac-vlan command is used to delete all VLANs based on the source MAC address.
The no mac-vlan mac <mac-address> command is used to delete a VLAN based on the source MAC address.

Examples
Create mac 0000.0000.0111 vlan 2 based on.

```
Switch#con t
Switch(config)#vlan database
Switch(config-vlan)#mac-vlan mac 0.0.0111 vlan 2
```

mac-vlan enable

Command

```
mac-vlanenable
```

Mode
Interface configuration mode

Parameters
None.

Description
The mac-vlanenable command is used to enable the MAC-VLAN function of the interface.

Examples
Start MAC-VLAN function on port ge1/1.

```
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#mac-vlan enable
```

mac-vlan disable

Command

```
mac-vlandisable
```

Mode
Interface configuration mode

Parameters
None.

Description
The mac-vlandisable command is used to disable the MAC-VLAN function of the interface.

Examples

```
#Disable the MAC-VLAN function of port ge1/1.
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#mac-vlan disable
```

show mac-vlan

Command

```
show mac-vlan
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
Displays information about the VLAN based on the source MAC address.

Examples
View the current mac-vlan configuration.

```
Switch#show mac-vlan
mac vlan table:
ifname ge1/1, mac 0000.0000.0111, vid 2
mac vlan table num: 1
Switch#
```

ip-subnet-vlan

Command

```
ip-subnet-vlan ip<ip-address><ip-mask> vlan <vlanid>
no ip-subnet-vlan ip<ip-address>< ip-mask>
no ip-subnet-vlan
```

Mode
vlan configuration mode

Parameters
ip-address:ip address
ip-mask: ip mask
vlan-id: The range of VLAN ID is 1-4094. vlan-id needs to be added first.

Description
ip-subnet-vlan ip<ip-address><ip-mask> vlan <vlanid> Create a VLAN based on the source IP subnet
no ip-subnet-vlan ip<ip-address><ip-mask> Deletes a VLAN based on the source IP subnet
no ip-subnet-vlan removes all VLANs based on the source IP subnet

Examples

```
#No
```

ip-subnet-vlanenable

Command

```
ip-subnet-vlanenable
```

Mode
Interface configuration mode

Parameters
None.

Description
The ip-subnet-vlanenable command is used to enable the ip-subnet-vlan function of an interface.

Examples

```
#start ip-subnet-vlan function for port ge1/1.
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)# ip-subnet-vlan enable
```

ip-subnet-vlandisable

Command

```
ip-subnet-vlandisable
```

Mode
Interface configuration mode

Parameters
None.

Description
The ip-subnet-vlandisable command is used to disable the ip-subnet-vlan function of an interface.

Examples
```
#Disable ip-subnet-vlan function on port ge1/1.
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)# ip-subnet-vlandisable
```

show ip-subnet-vlan

Command
```
show ip-subnet-vlan
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
Show all VLANs based on the source IP subnet

Examples
View the current configuration of the ip subnet.
```
Switch#sh ip-subnet-vlan
ip subnet vlan table:
ifname ge1/1, ip 192.168.0.2 255.255.255.255, vid 1
ip subnet vlan table num: 1
```

protocol-vlan ether-type

Command
```
protocol-vlan ether-type {arp | ip|ipv6|pppdiscovery | pppsession | <protocol-id> }vlan<vlan-id>
no protocol-vlan
no protocol-vlan ether-type {arp | ip|ipv6|pppdiscovery | pppsession | < protocol-id> }
```

Mode
Interface configuration mode

Parameters
vlan-id: The range of VLAN ID is 1-4094. vlan-id needs to be added first.
protocol-id: protocol number, in the range 0-65535

Description
The protocol-vlan ether-type<protocol-type> vlan <vlan-id> command is used to create a protocol-based VLAN.
The no protocol-vlan command is used to remove all protocol-based VLANs.
The no protocol-vlan ether-type<protocol-type> command is used to delete the VLAN based on the corresponding protocol.

Examples
Configure port ge1/1 protocol arp with packets belonging to VLAN2.
```
Switch(config-ge1/1)#protocol-vlan ether-type arp vlan 2
```

show protocol-vlan

Command
```
show protocol-vlan
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
Displays information about protocol-based VLANs.

Examples
View the current vlan division.

```
Switch#show protocol-vlan
protocol vlan table:
ethernet type 123, vid 100
ethernet type 3, vid 100
Switch#
```

show vlan-partition interface

Command

```
showvlan-partition interface<if-name>
```

Mode
Normal mode / Privilege mode

Parameters
if-name The specific interface name.

Description
Displays a specific port based on source MAC and protocol VLAN enablement.

Examples
Show source-based MAC and protocol VLAN enablement for port ge1/1

```
Switch#show vlan-partition interface ge1/1
mac vlan enable
ip subnet vlan enable
Switch#
```

vlan mapping command

vlan-mapping vlan

Command

```
vlan-mapping vlan <vlan-id> map-vlan <vlan-id>
no vlan-mapping [vlan<vlan-id>]
```

Mode
Interface configuration mode

Parameters
vlan-id: The vlan number to be displayed, in the range of 1-4094.

Description
Configure vlan-mapping mapping.

Examples
Configure vlan mapping.

```
Switch(config)#vlan-mapping vlan 1000 map-vlan 100
Switch(config)#
```

vlan-mapping enable

Command

```
vlan-mapping enable
```

Mode

Interface configuration mode

Parameters

None.

Description

Start the VLAN mapping relationship of the port.

Examples

```
VLAN mapping relationship for #start port ge1/1.
Switch#
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#vlan-mapping enable
Switch(config-ge1/1)#
```

vlan-mapping disable

Command

```
vlan-mapping disable
```

Mode

Interface configuration mode

Parameters

None.

Description

Turn off the VLAN mapping relationship of the port.

Examples

Close the VLAN mapping relationship for port ge1/1.

```
Switch#
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#vlan-mapping disable
Switch(config-ge1/1)#
```

show vlan-mapping

Command

```
show vlan-mapping
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

Displays the VLAN mapping configured for all interfaces.

Examples

View vlan mapping.

```
Switch#show vlan-mapping
Switch#
```

voice vlan command

voice-vlan oui

Command

```
voice-vlan oui <oui-address> mask <oui-mask> [description<string> ]
no voice-vlan oui <oui-address> mask <oui-mask>
no voice-vlan oui [ description<string>]
```

Mode

Global configuration mode

Parameters

The oui-address format is HHHH.HHHH.
The oui-mask format is also HHHH.HHHH.HHHH with oui-address together, 1 is required to match, 0 is not required to match.
string Naming information.

Description

The voice-vlan oui command is used to manually add oui table entries and can add descriptions.
The no voice-vlan oui <oui-address> mask <oui-mask> command is used to delete a specific oui table entry.
The no voice-vlan oui command removes all user-added oui table entries. If the description keyword is appended, a specific oui table is deleted.

Examples

Add oui table entries.

```
Switch(config)#voice-vlan oui 00e3.2233.0002 mask ffff.ff00.0000 description abc
Switch(config)#)#no voice-vlan oui
Switch(config)#)# no voice-vlan oui 00e3.2233.0002 mask ffff.ff00.0000
Switch(config)#)# no voice-vlan description abc
```

voice-vlan default-oui resume

Command

```
voice-vlan default-oui resume
```

Mode

Global configuration mode

Parameters

None.

Description

Restore all defualt OUI configurations.

Examples

```
#Restore all defualt OUI configurations.
Switch(config)#voice-vlan default-oui resume
```

no voice-vlan default-oui

Command

```
no voice-vlan default-oui <oui-address> mask <oui-mask>
no voice-vlan default-oui [ description<string>]
```

Mode

Global configuration mode

Parameters

The oui-address format is HHHH.HHHH.

The oui-mask format is also HHHH.HHHH.HHHH with oui-address together, 1 is required to match, 0 is not required to match.
string Naming information.

Description
The no voice-vlan default-oui <oui-address> mask <oui-mask> command is used to remove the specific default oui table entry.
The no voice-vlan default-oui command removes all default oui table entries. Followed by the description keyword to delete the specific oui.

Examples
```
#delete all defualt OUI configuration FF1A
Switch(config)#no voice-vlan default-oui
```

show voice-vlan oui

Command
```
show voice-vlan oui
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
Show all defualt with user OUI configuration

Examples
Show all OUI configurations.
```
Switch>show voice-vlan oui
oui address mask description
0001.e300.0000 ffff.ff00.0000 Siemens-phone
0003.6b00.0000 ffff.ff00.0000 Cisco-phone
0004.0d00.0000 ffff.ff00.0000 Avaya-phone
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone
0060.b900.0000 ffff.ff00.0000 Philips/NEC-phone
00e0.7500.0000 ffff.ff00.0000 Polycom-phone
00e0.bb00.0000 ffff.ff00.0000 3com-phone
Switch>
```

voice vlan

Command
```
voice vlan<vlan-id> {enable | disable }
```

Mode
Interface configuration mode

Parameters
vlan-id: The range of VLAN ID is 1-4094.

Description
Interface enable de-enables the VOICE vlan.

Examples
```
#Interface enable voice vlan 2.
Switch(config-ge1/1)#voice vlan 2 enable
Switch(config-ge1/1)#
```

voice vlan qos remark

Command

```
voice vlan qos remark cos<cos-value> dscp < dscp-value>
```

Mode

Interface configuration mode

Parameters

cos-value: the range of queue value is 0-7. default is 6.
dscp-value: The range of dscp value is 0-63. The default is 46.

Description

After setting the interface to match the VOICE vlan, modify the cos and dscp values of the matched messages.

Examples

Set interface remarkcos to 3 and dscp value to 63.

```
Switch(config-ge1/1)#voice vlan qos remark cos 3 dscp 63
Switch(config-ge1/1)#
```

no voice vlan qos

Command

```
no voice vlan qos
```

Mode

Interface configuration mode

Parameters

None.

Description

Restores the interface qos priority default configuration.

Examples

```
#No
```

no voice vlan

Command

```
no voice vlan
```

Mode

Interface configuration mode

Parameters

None.

Description

Delete all relevant configurations of the interface configuration Voice VLAN.

Examples

```
#No
```

show voice-vlan

Command

```
show voice-vlan
```

Mode

Normal mode / Privilege mode

Parameters
None.

Description
Displays all interfaces configured with Voice VLANs.

Examples
```
switch#show voice-vlan
voice vlan enable port:
port voice-vlan voice-cos voice-dscp
ge1/1 2 7 63
ge1/2 3 6 46
```

QinQ commands

qinq tpid

Command
```
qinq tpid<hex-tpid>
no qinq tpid
```

Mode
Interface configuration mode

Parameters
hex-tpid: set the global tpid value, hexadecimal number. The default is 8100.

Description
Modify the tpid value.

Examples
Configure port ge1/1 with a tpid of 9100
```
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#qinq tpid 9100
Switch(config-ge1/1)#
```

qinq customer

Command
```
qinqcustomer
no qinqcustomer
```

Mode
Interface configuration mode

Parameters
None.

Description
Configure the port for qinq user mode.

Examples
Configure port ge1/1 as customer
```
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#qinq customer
Switch(config-ge1/1)#
```

qinq uplink

Command

```
qinq uplink
no qinq uplink
```

Mode

Interface configuration mode

Parameters

None.

Description

The marked port is the QinQ uplink port.
Example·s
Configure port ge1/1 as uplink
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#qinq uplink
Switch(config-ge1/1)#

qinq outer-vid

Command

```
qinq outer-vid <vlan-id>inner-vid <vlan-id>
no qinq outer-vid <vlan-id>[inner-vid <vlan-id>]
```

Mode

Interface configuration mode

Parameters

vlan-id: The vlan number to be displayed, in the range of 1-4094.

Description

Converts multiple VLAN IDs of the subscriber network into a particular VLAN ID of the SP network, thus enabling the flexible QinQ feature. This command takes effect on non-uplink ports.

Examples

Add a tag of 100 to the packet received on port ge1/1 with a tag of 500

```
Switch#con t
Switch(config)#int ge1/1
Switch(config-ge1/1)#qinq outer-vid 100 inner-vid 500
Switch(config-ge1/1)#
```

show qinq

Command

```
show qinq
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

Check the qinq-related configuration.

Examples

```
#
Switch#show qinq
ifname tpid dtag-mode outer-vid inner-vid
```

```
ge1/1 0x8100 customer 2 1
Switch#
```

CHAPTER 07

QOS

QOS Configuration Commands

qos dscp-map-qp

Command

```
qos dscp-map-qp <dscp-value> qosprofile <qp-value>
no qos dscp-map-qp <qp-value>
```

Mode

Interface configuration mode.

Parameters

dscp-value: the value of dscp, in the range of 0-63
qp-value: the pair of packets,the values are qp0,qp1,qp2,qp3,qp4,qp5,qp6,qp7.

Description

The qos dscp-map-qp command indicates that the value of dscp is mapped to the pair column.
The no qos dscp-map-qp command restores to the default mapping.

Examples

Configure port ge1/1 dscp with a value of 50 to map to pair qp1.

```
Switch(config-ge1/1)#qos dscp-map-qp 50 qosprofile qp1
```

qos qosprofile

Command

```
qos qosprofile <qp-value> weight <weitht>
no qos qosprofile <qp-value> weight
```

Mode

Interface configuration mode.

Parameters

qp-value: the pair of packets,the values are qp0,qp1,qp2,qp3,qp4,qp5,qp6,qp7.
Weight:Indicates the value of the pair of column packets.

Description

The qos qosprofile command configures the pair of column weight values.
The no qos qosprofile command configures the column weight value to revert to the default value.

Examples

Configure port ge1/1 to have a weight of 50 for column qp1.

```
Switch(config-ge1/1)#qos qosprofile qp1 weight 50
Switch(config-ge1/1)#
```

qos sched

Command

```
qos sched { rr | sp | wrr |wdrr}
```

Mode

Interface configuration mode.

Parameters
RR: Round robin scheduling algorithm
SP: Strict priority scheduling algorithm
WRR: weighted round robin scheduling algorithm
WDRR: Enhanced WRR scheduling algorithm

Description
qos sched configures the QOS scheduling algorithm. The default is WRR.

Examples
Configure port ge1/1 to use SP strict priority scheduling algorithm.

```
Switch(config-ge1/1)#qos sched sp
```

qos dscp-based

Command

```
qos dscp-based
no qos dscp-based
```

Mode
Interface configuration mode.

Parameters
None.

Description
The qos dscp-based command configures dscp-based qos.
The no qos dscp-based command cancels qos.

Examples
Configure dscp-based qos on port ge1/1.

```
Switch(config-ge1/1)#qos dscp-based
Switch(config)#
```

qos user-priority

Command

```
qos user-priority <pri-value>
no qos user-priority
```

Mode
Interface configuration mode.

Parameters
Pri-value: the value of the priority.

Description
The qos user-priority command indicates the value of the cos used without the tag packet.
The no qos user-priority command restores to the default value.

Examples
Configure the value of user-priority to 5 on port ge1/1.

```
Switch(config-ge1/1)#qos user-priority 5
```

QOS View Command

show qos

Command

```
show qos
```

Mode

Normal mode/privileged mode.

Parameters

None.

Description

The show qos command displays global qos configuration information.

Examples

```
Switch#sh qos
Interface ge1/1
DSCP-Based QoS : Disable
Default Priority : 0/QP0
DSCP-Based QoS     : Disable
Default Priority   : 0/QP0
Priority Queues    : 8
Schedule Algorithm :  WRR(Weighted round robin)
Weight of Queues   : QP0[1],QP1[2],QP2[4],QP3[8],QP4[16],QP5[32],QP6[64],QP7[127]
COS map QosProfile : COS0[QP0],COS1[QP1],COS2[QP2],COS3[QP3],COS4[QP4],COS5[QP5],COS6[QP6],COS7[QP7]
DSCP map QosProfile:
DSCP0-DSCP7[QP0],DSCP8-DSCP15[QP1],DSCP16-DSCP23[QP2],DSCP24-DSCP31[QP3],DSCP32-DSCP39[QP4],DSCP40-DS
CP47[QP5],DSCP48-DSCP55[QP6],DSCP56-DSCP63[QP7]
QoS Profile Configuration :
QP0 Priority[0] Queue[0]
QP1 Priority[1] Queue[1]
QP2 Priority[2] Queue[2]
QP3 Priority[3] Queue[3]
QP4 Priority[4] Queue[4]
QP5 Priority[5] Queue[5]
QP6 Priority[6] Queue[6]
QP7 Priority[7] Queue[7]
```

show qos interface

Command

```
show qos interface [if-name]
```

Mode

Normal mode/privileged mode.

Parameters

if-name: Interface name.

Description

Show qos interface command to view information about port qos.

Examples

```
Switch#sh qos ge1/1
Interface ge1/1
DSCP-Based QoS : Disable
Default Priority : 0/QP0
Priority Queues : 8
```

```
Schedule Algorithm : WRR(Weighted round robin)
Weight of Queues : QP0[1],QP1[2],QP2[4],QP3[8],QP4[16],QP5[32],QP6[64],QP7[127]
COS map QosProfile : COS0[QP0],COS1[QP1],COS2[QP2],COS3[QP3],COS4[QP4],COS5[QP5],COS6[QP6],COS7[QP7]
DSCP map QosProfile: DSCP0-DSCP7[QP0], DSCP8-DSCP15[QP1], DSCP16-DSCP23[QP2], DSCP24-DSCP31[QP3],
DSCP32-DSCP39[QP4], DSCP40-DSCP47[QP5], dscp48-dscp55[qp6],dscp56-dscp63[qp7]
QoS Profile Configuration :
QP0 Priority[0] Queue[0]
QP1 Priority[1] Queue[1]
QP2 Priority[2] Queue[2]
QP3 Priority[3] Queue[3]
QP4 Priority[4] Queue[4]
QP5 Priority[5] Queue[5]
QP6 Priority[6] Queue[6]
QP7 Priority[7] Queue[7]
```

Policy QOS commands

qos class

Command

```
qos class <class-id> name <class-name>
qos class <class-id> match acl <acl-list>
qos class <class-id> match cos<cos-value1><cos-value2>...
qos class <class-id> match dscp<dscp-value1><dscp-value2>...
no qos class <class-id>
```

Mode

Global configuration mode

Parameters

class-id: class id takes values in the range <1-256>.
class -name: class name Character length <1-32>.
acl-list: access list globally configured acl rules, only 1 group of rules can be configured at a time.
cos-value: Define the matching 802.1p priority rule, 8 cos values can be configured at the same time.
dscp-value: Define the matching DSCP rule, 8 dscp values can be configured at the same time.

Description

The qos class <class-id> name <class-name> command is used to name the specified class.
Define class and define a set of flow classification rules: there are three flow classification rules in total, 802.1p priority, DSCP, and ACL. A class can only use one set of flow classification rules, and a set of flow classification rules can be used by multiple classes. The default configuration does not match any rules.
The no qos class <class-id> command is used to delete the configuration corresponding to the class-id.

Examples

```
Switch(config)#qos class 3 name net3
Switch(config)#
#define class 3 match cos 1, 2, 3
Switch(config)#qos class 3 match cos 1 2 3
Switch(config)#
```

show qos class

Command

```
show qos class [<class-id>]
```

Mode

Normal mode / Privilege mode

Parameters
class-id: class id takes values in the range <1-256>.

Description
Query the configuration of the qos class

Examples
```
#query qos class
Switch#show qos class
class 3: name net3, match cos 1 2 3
Switch#
```

qos policy

Command
```
qos policy<policy -id> name <policy -name>
[no] qos policy <policy -id> class <class-id> meter <rate>
[no] qos policy <policy -id> class <class-id>mirror-to { cpu | monitor-interface}
[no] qos policy <policy -id> class <class-id>remark cos <cos-value>
[no] qos policy <policy -id> class <class-id>remark dscp <dscp-value>
[no] qos policy <policy -id> class <class-id>statistic-packets
[no]qos policy <policy -id> class <class-id>map-queue<queue-id>
no qos policy <policy -id> [class <class-id>]
```

Mode
Global configuration mode

Parameters
policy -id: policy id Takes values in the range <1-256>.
policy -name: policy name Character length <1-32>.
class-id: class id takes values in the range <1-256>.
rate :Rate limit.
queue-id: mapping to the corresponding queue, takes the value 0-7.
dscp-value: the DSCP priority value of the re-tagged message.

Description
The qos policy< policy -id> name <policy -name> command is used to give a name to the specified policy.
The qos policy < policy -id> class <class-id> meter command is used to give the specified class the corresponding speed limit.
The keyword mirror-to is used to mirror the specified class. The keyword remark is used to modify the corresponding priority of the specified class of messages. The keyword statistic-packets is used to give statistics to the specified class of messages.

Examples
```
Switch(config)# qos policy 2 class 3 remark dscp 33
Switch(config)# qos policy 2 class 3 statistic-packets
```

clear interface

Command
```
clear interface <if-name> qos policy statistic-packets
```

Mode
Privilege mode

Parameters
if-name: The specific physical interface.

Description
Clear the statistics of the interface qos policy.

Examples

```
#No
```

qos apply-policy

Command

```
qos apply-policy<policy-id>
no qos
```

Mode

Interface configuration mode

Parameters

policy-id: policy id takes values in the range <1-256>.

Description

Enable the policy QoS function of the interface

Examples

```
#No
```

show qos policy

Command

```
show qos policy [<policy-id>]
```

Mode

Normal mode / Privilege mode

Parameters

policy-id: policy id takes values in the range <1-256>.

Description

Query the configuration of qos policy

Examples

```
#query qos policy
Switch#show qos policy
policy 2: name net3
class 3: remark dscp 33, statistic packets,
Switch#
```

CHAPTER 08

MSTP commands

MSTP configuration commands

spanning-tree mst cisco-interoperability

Command

```
spanning-tree mst cisco-interoperability {disable | enable}
```

Mode

Global configuration mode

Parameters

disable: disable the function. Disable by default.
enable: Turn on the function.

Description

Enable or disable compatibility with cisco's Spanning Tree Protocol.
The switch uses 802.1s-based MSTP protocol with a length of 16 bytes per MSTI message, while the CISCO switch's BPDUs have a length of 26 bytes per MSTI message. In order to be used with CISCO switches, the switch should be configured with CISCO compatible switches enabled.

Examples

```
None.
```

spanning-tree mst configuration

Command

```
spanning-tree mst configuration
```

Mode

Global configuration mode

Parameters

None

Description

Enter the configuration mode of spanning-tree.

Examples

```
None.
```

spanning-tree mst enable

Command

```
spanning-tree mst enable
```

Mode

Global configuration mode

Parameters

None

Description

Start mstp calculation.

Examples

None.

spanning-tree mst errdisable-timeout

Command

```
spanning-tree mst errdisable-timeout {enable | interval <seconds>}
no spanning-tree mst errdisable-timeout {enable | interval}
```

Mode

Global configuration mode

Parameters

seconds: timeout time, range 10-1000000 seconds. Default is 300 seconds.

Description

The spanning-tree mst errdisable-timeout enable command starts the errdisable mechanism, which starts the errdisable timer when the port that started the BPDU gurad receives a BPDU. errdisable restarts after the system-configured timeout period This port.
The spanning-tree mst errdisable-timeout interval command sets the errordisable timeout interval.
The no spanning-tree mst errdisable-timeout command is used to cancel the corresponding configuration and restore the default value.

Examples

None.

spanning-tree mst forward-time

Command

```
spanning-tree mst forward-time <seconds>
no spanning-tree mst forward-time
```

Mode

Global configuration mode.

Parameters

seconds: the number of seconds the port waits from discarding to learning and learning to forwarding. The range is 4-30 seconds. Default is 15 seconds.
According to the generation number protocol forward-time must meet the following conditions.
2*(forward-time - 1) >= max-age.

Description

The spanning-tree mst forward-time command is used to configure the forwarding delay time.
The no spanning-tree mst forward-time command is used to cancel the forwarding delay configuration and restore the default value.

Examples

None.

spanning-tree mst hello-time

Command

```
spanning-tree mst hello-time <seconds>
no spanning-tree mst hello-time
```

Mode

Global configuration mode

Parameters

seconds: The interval between configuration messages generated by the root switch. The range is 1-10 seconds. Default 2 seconds.

According to the generation number protocol hello-time must satisfy the following conditions.
2*(hello-time + 1) =< max-age.

Description
spanning-tree mst hello-time Configure the interval between sending MSTP hello messages.
The no spanning-tree mst hello-time command cancels the configuration and restores the default value.

Examples
Configure hello messages to be sent at an interval of 10 seconds.

```
Switch(config)#spanning-tree mst hello-time 10
Switch(config)#
```

spanning-tree mst max-age

Command

```
spanning-tree mst max-age <seconds>
no spanning-tree mst max-age
```

Mode
Global configuration mode

Parameters
seconds: The number of seconds the switch waits to receive Spanning Tree configuration information before triggering a reconfiguration. The range is 6-40 seconds. The default is 20 seconds.

Description
Configure the maximum time to listen to the root bridge.
The no command cancels the configuration and restores the default value.

Examples

```
None.
```

spanning-tree mst max-hops

Command

```
spanning-tree mst max-hops <hops>
no spanning-tree mst max-hops
```

Mode
Global configuration mode

Parameters
hops: the number of hops specified in a domain before the BPDU is dropped. The range is 1-40. 20 hops is the default.

Description
Configure the maximum number of hops for which BPDU protocol packets are valid.
The no command cancels the configuration and restores the default value.

Examples

```
None.
```

spanning-tree mst portfast

Command

```
spanning-tree mst portfast
no spanning-tree mst portfast
```

Mode
Interface configuration mode

Parameters
None

Description

The spanning-tree mst portfast command configures a port as a portfast port, which enables the port to go from the blocking state to the forwarding state, bypassing the listening and learning states.
The no command cancels the configuration and restores the default value.

Examples

Configure port ge1/1 as portfast interface.

```
Switch(config-ge1/1)#spanning-tree mst portfast
Switch(config-ge1/1)#
```

spanning-tree mst portfast bpdu-filter

Command

```
spanning-tree mst portfast bpdu-filter [default | disable | enable]
no spanning-tree mst portfast bpdu-filter
```

Mode

Global Configuration Mode/Interface Configuration Mode

Parameters

default: default state.
disable: Disable the function.
enable: enable the function.

Description

Prevents the portfast port from receiving or sending BPDUs.
In global configuration mode, the spanning-tree mst portfast bpdu-filter command enables the BPDU filtering function on ports in the portfast bpdu-filter default state. In interface configuration mode, spanning-tree mst portfast bpdu-filter enable turns on BPDU filtering on any port.
The no command cancels the configuration and restores the default value.

Examples

Configure port ge1/1 as portfast interface and not to send mstp bpdu packets.

```
Switch(config-ge1/1)#spanning-tree mst portfast
Switch(config-ge1/1)#spanning-tree mst portfast bpdu-filter enable
Switch(config-ge1/1)#
```

spanning-tree mst portfast bpdu-guard

Command

```
spanning-tree mst portfast bpdu-guard [default | disable | enable]
no spanning-tree mst portfast bpdu-guard
```

Mode

Global Configuration Mode/Interface Configuration Mode

Parameters

default: default state.
disable: Disable the function.
enable: enable the function.

Description

When a port configured with BPDU gurad receives a BPDU, the spanning tree will shutdown this port. In a valid configuration, a port fast-enabled port does not receive BPDUs. receiving a BPDU on a port fast enabled port indicates an invalid configuration, such as a connection from an unauthorized device, and the BPDU guard goes to an error-disabled state.
The no command cancels the configuration and restores the default value.

Examples

Configure port ge1/1 as portfast interface and enable BPDU protection.

```
Switch(config-ge1/1)#spanning-tree mst portfast
```

```
Switch(config-ge1/1)#spanning-tree mst portfast bpdu-guard enable
Switch(config-ge1/1)#
```

spanning-tree mst priority

Command

```
spanning-tree mst priority <value>
```

Mode

Global configuration mode

Parameters

value: priority of CIST bridge, range 0-61440, default value is 32768. the value of CIST priority can only be a multiple of 4096.

Description

Configure the bridge priority. Devices with a low bridge priority are more likely to be the root bridge.

Examples

Configure CIST bridge priority to 36862.

```
Switch#configure terminal
Switch(config)#spanning-tree mst priority 36862
Switch(config)#
```

instance

Command

```
instance <instance-id> [priority <value> | vlan <vlan-id>]
no instance <instance-id>[vlan <vlan-id>]
```

Mode

MSTP configuration mode

Parameters

instance-id: the instance number to be created, in the range 1-15.
value: value of priority, range 0-61440, granularity 4096. default value is 32768.
vlan-id: The vlan number added to the instance.

Description

The instance <instance-id> command creates an instance.
The instance <instance-id>priority <value> command configures the priority of the MSTI bridge.
The instance <instance-id> vlan <vlan-id> command adds an instance vlan.
The no instance <instance-id> command removes the instance.
The no instance <instance-id>vlan <vlan-id> command removes the association of a vlan with an instance.

Examples

Create MSTP instance 2, add vlan2, vlan3.

```
Switch(config-mst)#instance 2
Switch(config-mst)#instance 2 vlan 2
Switch(config-mst)#instance 2 vlan 3
Switch(config-mst)#
```

region

Command

```
region <region-name>
no region
```

Mode

MSTP configuration mode

Parameters
region-name: domain name of the MSTP domain, length 1-32 characters.
The no command cancels the domain name configuration.

Description
Configure the domain name.

Examples
```
None.
```

revision

Command
```
revision <revision-num>
```

Mode
MSTP configuration mode

Parameters
revision-num: revision number, range 0-255.

Description
Configure the revision number.

Examples
```
None.
```

spanning-tree mst force-version

Command
```
spanning-tree mst force-version <version>
no spanning-tree mst force-version
```

Mode
Interface configuration mode

Parameters
version: The type of the protocol, in the range 0-3. 0 stands for STP protocol, 1 stands for spanning tree not supported, 2 stands for RSTP protocol, and 3 stands for MSTP protocol. The default protocol type is 0.

Description
Configure the type of protocol packet to be sent.
The no command cancels the configuration and restores the default value.

Examples
Configure port ge1/1 to send stp protocol packets.
```
Switch(config-ge1/1)# spanning-tree mst force-version 0
Switch(config-ge1/1)#
```

spanning-tree mst guard root

Command
```
spanning-tree mst guard root
no spanning-tree mst guard root
```

Mode
Interface configuration mode

Parameters
None

Description

Configure the enable root guard function to not receive BPDU packets with higher bridge priority than yourself, and designate this switch as the root switch. The default is off.
The no command cancels the configuration and restores the default value.

Examples

```
None.
```

spanning-tree mst instance

Command

```
spanning-tree mst instance <instance-id>[path-cost <cost> | priority <value>]
no spanning-tree mst instance<instance-id>[path-cost <cost>]
```

Mode

Interface configuration mode

Parameters

instance-id: instance number. Range 1-15.
cost: path overhead value, range 1-200000000. lower path overhead is more likely to be the root. The default value is 20000000.
priority <value>: The value of the MSTI priority, in the range 0-240, and can only be a multiple of 16. Lower priority values are more likely to be the root.

Description

The spanning-tree mst instance <instance-id> command adds the interface to the instance.
The spanning-tree mst instance <instance-id>path-cost <cost> command sets the msti path overhead.
The spanning-tree mst instance <instance-id>priority <value> command sets the msti priority.
The no command cancels the configuration and restores the default value.

Examples

```
#Add port ge1/1 to instance 2 and configure the port with a path overhead of 10 and a priority of
160.
Switch(config-ge1/1)#spanning-tree mst ins 2 path-cost 10
Switch(config-ge1/1)#spanning-tree mst ins 2 priority 160
Switch#show spanning-tree mst instance 2 interface ge1/1
%   ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
%   ge1/1: Designated Internal Path Cost 0  - Designated Port Id 0
%   ge1/1: Configured Internal Path Cost 10
%   ge1/1: Configured CST External Path cost 20000000
%   ge1/1: CST Priority 128  - MSTI Priority 160
%   ge1/1: Designated Root 0000000000000207
%   ge1/1: Designated Bridge 0000000000000207
%   ge1/1: Message Age 0 - Max Age 0
%   ge1/1: Hello Time 0 - Forward Delay 0
%   ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
Switch#
```

spanning-tree mst link-type

Command

```
spanning-tree mst link-type { point-to-point | shared}
no spanning-tree mst link-type
```

Mode

Interface configuration mode

Parameters

point-to-point: The connection type is point-to-point, allowing fast port state transition. is the default type.
shared: The connection type is shared, which does not allow fast port state transition and has to go through the calculation process of 802.1D to determine the state of the port.

Description

Configure the connection type of the interface.
The no command cancels the configuration and restores the default value.

Examples

```
None.
```

spanning-tree mst path-cost

Command

```
spanning-tree mst path-cost <cost>
no spanning-tree mst path-cost
```

Mode

Interface configuration mode

Parameters

cost: cist path overhead value, range 1-200000000. default value 20000000. lower path overhead is more likely to be the root.
The following is the bandwidth and path spend mapping table.

Bandwidth(bps)	Paths to spend
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000 (10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000 (1T)	20
>1000000000000	2

Description

Configure cist path overhead.
The no command cancels the configuration and restores the default value.

Examples

Configure the cist path overhead for port ge1/1 in example 2 to 200.

```
Switch(config-ge1/1)#spanning-tree mst path-cost 200
Switch#show spanning-tree mst instance 2 interface ge1/1
% ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% ge1/1: Configured Internal Path Cost 20000000
% ge1/1: Configured CST External Path cost 200
% ge1/1: CST Priority 128 - MSTI Priority 128
% ge1/1: Designated Root 0000000000000207
% ge1/1: Designated Bridge 0000000000000207
% ge1/1: Message Age 0 - Max Age 0
% ge1/1: Hello Time 0 - Forward Delay 0
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
Switch#
```

spanning-tree mst priority

Command

```
spanning-tree mst priority <value>
```

Mode
Interface configuration mode

Parameters
value: priority of the cist port, range 0-240, can only be a multiple of 16. The default value is 128.

Description
Configure the cist priority of the interface.

Examples
Configure the cist priority of instance 2 port ge1/1 to 240.

```
Switch(config-ge1/1)#spanning-tree mst priority 240
Switch#show spanning-tree mst instance 2 interface ge1/1
% ge1/1: Port 2001 - Id f7d1 - Role Disabled - State Forwarding
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% ge1/1: Configured Internal Path Cost 10
% ge1/1: Configured CST External Path cost 20000000
% ge1/1: CST Priority 240 - MSTI Priority 160
% ge1/1: Designated Root 0000000000000207
% ge1/1: Designated Bridge 0000000000000207
% ge1/1: Message Age 0 - Max Age 0
% ge1/1: Hello Time 0 - Forward Delay 0
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
Switch#
```

clear spanning-tree detected protocols

Command

```
clear spanning-tree detected protocols [interface <if-name>]
```

Mode
Privilege mode

Parameters
if-name: The port that needs to reset the STP protocol reconnaissance function.

Description
For compatibility with 802.1D STP protocols, the system can automatically reconnoitre the protocols running on the other system and determine the protocols running on this port based on the protocols running on the other system. clear spanning-tree detected protocols command resets this protocol negotiation task to let it renegotiate the protocols between it and the host.

Examples

```
#Disable STP protocol reconnaissance on module 1 port 1.
Switch#clear spanning-tree detected protocols interface ge1/1
switch#
```

8.2 MSTP View Command

8.2.1 show spanning-tree mst

Command

```
show spanning-tree mst [config | detail | instance <instance-id> [interface <if-name>] | interface
<if-name>]
```

Mode
Normal mode / Privilege mode

Parameters
instance-id: instance number, range 0-15.
if-name: Interface number.

Description

The show spanning-tree mst command displays cist information and the corresponding table of vlan and instance.
The show spanning-tree mst config command displays the configuration information of mstp.
The show spanning-tree mst detail command displays detailed information about mstp, including cist interface information, instance information, and instance interface information.
The show spanning-tree mst instance <instance-id> command displays information about an instance.
The show spanning-tree mst instance <instance-id>interface <if-name> command displays information about a cist interface.
show spanning-tree mst interface <if-name>: Displays information about an msti interface.

Examples

Display mstp configuration information.

```
Switch#show spanning-tree mst config
%
% MSTP Configuration Information for bridge 1.
%-------------------------------------------------------
% Format Id : 0
% Name :
% Revision Level :1
% Digest : 0xD042DCDBBC60C63B623C157F60A37A6F
%-------------------------------------------------------
```

Display mstp information for interface ge1/1 within instance 1.

```
Switch#show spanning-tree mst instance 1 interface ge1/1
% ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Discarding
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% ge1/1: Configured Internal Path Cost 20000000
% ge1/1: Configured CST External Path cost 20000
% ge1/1: CST Priority 128 - MSTI Priority 128
% ge1/1: Designated Root 0000000000000000
% ge1/1: Designated Bridge 0000000000000000
% ge1/1: Message Age 0 - Max Age 0
% ge1/1: Hello Time 0 - Forward Delay 0
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
Switch#
```

8.3 MSTP debugging commands

8.3.1 debug mstp

Command

```
debug mstp
no debug mstp
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp command is used to turn on the debug switch related to the mstp protocol and write the related logs to the log table.
The no debug mstp command disables the debug switch of mstp.

Examples

```
#Turn on mstp debug switch
Switch#debug mstp
```

```
Switch#
```

8.3.2 debug mstp all

Command

```
debug mstp all
no debug mstp all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp all command is used to turn on all mstp protocol-related debug switches and write the related logs to the log table.
The no debug mstp all command disables the debug switch of mstp.

Examples

Turn on all debug switches for the mstp protocol.

```
Switch#debug mstp all
Switch#
```

8.3.3 debug mstp cli

Command

```
debug mstp cli
no debug mstp cli
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp cli command is used to turn on the mstp protocol-related command debug switch and write the related logs to the log table.
The no debug mstp cli command disables the command debug switch of mstp.

Examples

Turn on the mstp protocol command debug switch.

```
Switch#debug mstp cli
Switch#
```

8.3.4 debug mstp packet

Command

```
debug mstp packet [recv | send]
no debug mstp packet [recv | send]
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp packet command is used to turn on the debug switch for mstp protocol packets and write the related logs to the log table.
The no debug mstp packet command is used to disable the mstp packet debug switch.

Examples

Turn on the mstp protocol message reception debug switch.

```
Switch#debug mstp packet recv
Switch#
```

8.3.5 debug mstp protocol

Command

```
debug mstp protocol [detail]
no debug mstp protocol [detail]
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp protocol command is used to turn on the debug switch for mstp protocol messages and write the related logs to the log table.

The no debug mstp protocol command is used to turn off the mstp message debugging switch.

Examples

Turn on the mstp protocol detailed debug switch.

```
Switch#debug mstp protocol detail
Switch#
```

8.3.6 debug mstp timer

Command

```
debug mstp timer [detail]
no debug mstp timer [detail]
```

Mode

Privilege mode.

Parameters

None.

Description

The debug mstp timer command is used to turn on the timer debug switch of mstp protocol and write the related logs to the log table.

The no debug mstp timer command is used to turn off the timer debug switch of mstp.

Examples

Turn on the mstp protocol timer debug switch.

```
Switch#debug mstp timer detail
Switch#
```

CHAPTER 09

EAPS command

Configuration commands

eaps control-vlan

Command

```
eaps control-vlan<ring-id><vlan-id>
no eaps control-vlan<ring-id>
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.
vlan-id: control vlan ID number, range 2-4094.

Description

Configure the control vlan for the specified EAPS ring. the control vlan is only used to transmit EAPS protocol packets and can only contain two ports, primary port and secondary port.
The no command removes the control vlan configuration.

Examples

```
Configure the control vlan for EAPS ring 1 to be vlan2.
Switch(config)#eaps control-vlan 1 2
```

eaps create

Command

```
eaps create<ring-id>
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.

Description

Creates an EAPS ring with the specified ID number.

Examples

```
Create EAPS ring 1.
Switch (config)#eaps create 1
```

eaps disable

Command

```
eaps disable<ring-id>
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.

Description
Closes the EAPS ring for the specified ID number. The configuration is retained after shutdown.

Examples
```
Close EAPS 1.
Switch(config)#eaps disable 1
```

eaps enable

Command
```
eaps enable<ring-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.

Description
Enables the EAPS ring with the specified ID number.

Examples
```
Enables EAPS 1.
Switch(config)#eaps enable 1
```

eaps extreme-interoperability

Command
```
eaps extreme-interoperability<ring-id> {disable | enable}
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.

Description
Configure whether the EAPS ring with the specified ID number is compatible with Extreme devices. If compatible mode is selected, the protocol packet will be encapsulated in the same way as the Extreme device. If incompatible mode is selected, the protocol packet is encapsulated in the same way as specified in RFC3619. Extreme compatibility mode is turned on by default.

Examples
```
Disable EAPS Ring 1 compatibility with Extreme devices.
Switch(config)#eaps extreme-interoperability 1 disable
```

eaps fail-time

Command
```
eaps fail-time<ring-id><fail-time>
no eaps fail-time<ring-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.
fail-time: ring failure time, range 2-65535 seconds, default is 3 seconds.

Description
Configure the ring fail-time for the specified EAPS ring. If no Health packets are received within the fail-time, the ring is considered broken and the secondary port of the Master node is opened. In an EAPS ring, only the master node has this configuration in effect.

The no command restores fail-time to its default setting.

Examples

```
Configure the fail-time of EAPS 1 to 9 seconds.
Switch(config)#eaps fail-time 1 9
```

eaps hello-time

Command

```
eaps hello-time<ring-id><hello-time>
no eaps hello-time<ring-id>
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.
Hello-time: the interval time for the Master node to send out Health packets, ranging from 1-65535 seconds, default is 1 second.

Description

Configure the interval between EAPS HEALTH packets being sent out. In an EAPS ring, this configuration takes effect only for the Master node. Configuration condition: hello-time < fail-time.
The no command restores hello-time to its default setting.

Examples

```
Configure EAPS 1 to send out Health packets at an interval of 6 seconds.
Switch(config)#eaps hello-time 1 6
```

eaps mode

Command

```
eaps mode<ring-id> {master | transit}
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.

Description

Configure the role of the device in the specified EAPS ring. The master is responsible for checking loop integrity and blocking ports to prevent loops. There can be only one master in an EAPS ring, and there can be multiple transits.

Examples

```
Configure the device's role in EAPS 1 as master.
Switch(config)#eaps mode 1 master
```

eaps primary-port

Command

```
eaps primary-port<ring-id><if-name>
no eaps primary-port<ring-id>
```

Mode

Global configuration mode

Parameters

ring-id: ID number of the EAPS ring, range 1-16.
if-name: port name, can be physical port and link aggregation port.

Description
Configure the EAPS ring master port of the device. The primary port must be a tag port, a tag member of the control vlan and the protection vlan.
The no command removes the PRIMARY port for the specified ring.

Examples
```
Specify the primary port of EAPS 1 as ge1/1.
Switch(config)#eaps primary-port 1 ge1/1
```

eaps protected-vlan

Command
```
eaps protected-vlan<ring-id><vlan-id>
no eaps protected-vlan<ring-id><vlan-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.
vlan-id: ID number of the protection vlan of this EAPS ring.

Description
Configure the protection vlan of the specified EAPS ring. the EAPS ring can prevent its protection vlan from forming a loop.
The no command removes the specified protection vlan for the specified EAPS ring.

Examples
```
Configure the protection vlan of EAPS 1 as vlan3, vlan4.
Switch(config)#eaps protected-vlan 1 3
Switch(config)#eaps protected-vlan 1 4
```

eaps remove

Command
```
eaps remove<ring-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.

Description
Delete the configuration of the EAPS ring with the specified ID number. Turn off this EAPS ring before deleting it.

Examples
```
Delete EAPS 1.
Switch(config)#eaps remove 1
```

eaps secondary-port

Command
```
eaps secondary-port<ring-id><if-name>
no eaps secondary-port<ring-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.
if-name: port name, can be physical port and link aggregation port.

Description
Configure the EAPS domain slave port of the device. The slave port must be a tag port, a tag member of the control vlan and the protection vlan.
The no command removes the secondary port of the specified ring.

Examples
```
Configure the slave port of EAPS 1 as ge1/2.
Switch(config)#eaps secondary-port 1 ge1/2
```

eaps data-span

Command
```
eaps data-span<ring-id>
```

Mode
Global configuration mode

Parameters
ring-id: ID number of the EAPS ring, range 1-16.

Description
Configure the device to share data in the specified EAPS ring.

Examples
Configure devices to share data in EAPS ring 1.
```
Switch(config)# eaps data-span1
```

View command

show eaps

Command
```
show eaps [<ring-id>]
```

Mode
Normal mode / Privilege mode

Parameters
ring-id: ID number of the configured EAPS ring, range 1-16.

Description
If you do not enter the ring-id parameter, the number of currently configured eaps rings and their enablement are displayed.
Specifying ring-id displays the specifics of the eaps ring.

Examples
```
Switch#show eaps
eaps enable 1
eaps disable 2
Switch#show eaps 1
% EAPS Ring 1 - enable, Version 1, Mode - Master, State - Complete.
% Hello Time Interval - 1 secs, Current - on.
% Fail Time Age - 3 secs, Current - on.
% Pre-forwarding Time Age - 0 secs, Current - off.
% PortPrimary - ge1/5, State - Forwarding.
% PortSecondary - ge1/6, State - Blocking.
% Extreme interoperability admin - on, oper - on.
% Data spanning with rings - off.
Bridge% Id - 00:09:CA:88:03:05.
% Control Vlan ID - 2.
% Protected Vlan list - 1,3.
```

```
% BridgeLinkDownLast - 00:09:CA:77:02:C1.
```

Debugging commands

debug eaps

Command

```
debug eaps [all | events | packet [recv | send]]
no debug eaps [all | events | packet [recv | send]]
```

Mode

Privilege Mode

Parameters

all: Turn on all eaps related debug switches.
events: Turn on the debug switch for eaps event handling.
packet: Turn on the debug switch for eaps protocol packets.
recv: Turn on the receive eaps protocol messages debug switch only.
send: Turn on the send eaps protocol message debug switch only.

Description

The debug eaps command is used to turn on the eaps debug switch to enable users to see the eaps event processing and protocol messages sent and received.
The no debug eaps command is used to turn off the eaps debug switch.

Examples

```
Turn on the debug switch for the eaps protocol package at
Switch#debug eaps packet
Switch#log display
```

CHAPTER 10

ERPS command

Configuration commands

erps

Command

```
erps<domain-id>
no erps<domain-id>
```

Mode

Global configuration mode

Parameters

domain-id: ID number of the ERPS domain, in the range 1-8.

Description

The erps<domain-id> command is to create an ERPS instance.
The no erps<domain-id> command is to delete an ERPS instance

Examples

```
#Create ERPS ring example 1.
Switch(config)#erps 1
Switch(config-erps-1)#
```

erps predefine configuration

Command

```
erps predefine configuration <ring-node | rpl-owner-node >
```

Mode

Global Mode

Parameters

ring-node ring common node
rpl-owner-node ring-ownoer node

Description

ring-node A template for configuring a device as a ring common node
rpl-owner-node Template for configuring a device as a ring-ownoer node

Examples

Configure ERPS to configure one device in the ring as an ownoer node.

```
Switch#conf t
Switch(config)#
Switch(config)#erps predefine configuration rpl-owner-node
```

node-role

Command

```
node-role<interconnection | none - interconnection>
```

Mode

ERPS ring configuration mode

Parameters
None.

Description
The node-roleinterconnection command is to configure the role that the ERPS plays in the ring as an interconnection node.
The node-rolenone-interconnection command configures the role of ERPS in the ring to be a non-interconnection node, and the default role is non-interconnection node.

Examples
Configure the role that the ERPS plays in the ring as a non-interconnected node.

```
Switch(config)#erps 1
Switch(config-erps-1)#node-role none - interconnection
```

ring

Command

```
ring<ring-id>
no ring<ring-id>
```

Mode
ERPS ring configuration mode

Parameters
ring-id: ID number of the ERPS ring, range 1-32.

Description
The ring<ring-id> command is to create an ERPS ring.
The no ring<ring-id> command removes an ERPS ring.

Examples

```
#Create ERPS ring 32.
Switch(config)#erps 1
Switch(config-erps-1)#ring 32
Switch(config-erps-1)#
```

ring <1-32> ring-mode

Command

```
ring <1-32> ring-mode<major-ring|sub-ring>
```

Mode
ERPS ring configuration mode

Parameters
None

Description
The ring <1-32> ring-mode command is to configure whether the mode of the ERPS ring is primary or subring.
Where major-ring is the main-ring and sub-ring is the sub-ring.

Examples
Configure ERPS ring 32 as the main ring.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 ring-mode major-ring
Switch(config-erps-1)#
```

ring <1-32>node-mode

Command

```
ring <1-32>node-mode<ring-node|rpl-neighbor-node | rpl-owner-node>
```

Mode
ERPS ring configuration mode

Parameters
None

Description
The ring <1-32>node-mode command is to configure the node mode of the ERPS ring.
There are currently three node modes: RPL owner node, RPL neighbor node or normal link point.

Examples
Configure ERPS ring 32 node mode as RPL owner.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 node-mode rpl-owner-node
Switch(config-erps-1)#
```

ring <1-32>raps-vlan

Command

```
ring <1-32>raps-vlan <vlan-id >
no ring <1-32>raps-vlan <vlan-id>
```

Mode
ERPS ring configuration mode

Parameters
vlan-id:range is 2-4094

Description
The ring<1-32>raps-vlan command is to configure the ERPS ring protocol VLAN.
The no ring<1-32>raps-vlan command is to delete the ERPS ring protocol VLAN.

Examples
Configure ERPS ring 32 protocol VLAN to 2.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 raps-vlan 2
Switch(config-erps-1)#
```

ring <1-32>traffic-vlan

Command

```
ring <1-32>traffic-vlan<vlan-id >
no ring <1-32>traffic-vlan<vlan-id>
```

Mode
ERPS ring configuration mode

Parameters
vlan-id:range is 1-4094

Description
The ring<1-32>traffic-vlan command is to configure the ERPS ring data VLAN.
The no ring<1-32>traffic-vlan command is to delete the ERPS ring data VLAN.

Examples
Configure ERPS ring 32 protocol VLAN to 3.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32traffic-vlan3
Switch(config-erps-1)#
```

ring <1-32>rpl-port

Command

```
ring <1-32>rpl-port<if-name>
no ring <1-32>rpl-port
```

Mode

ERPS ring configuration mode

Parameters

if-name: port name, can be a physical port and a link aggregation port.

Description

The ring<1-32> rpl-port command is to configure the RPL port.
The no ring<1-32> rpl-port command is to delete the RPL port.

Examples

Configure the ring RPL port of ERPS ring 32 as ge1/1.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32rpl-portge1/1
Switch(config-erps-1)#
```

ring <1-32>rl-port

Command

```
ring <1-32>rl-port<if-name>
no ring <1-32>rl-port
```

Mode

ERPS ring configuration mode

Parameters

if-name: port name, can be a physical port and a link aggregation port.

Description

The ring<1-32> rl-port command is to configure the RL port.
The no ring<1-32> rl-port command is to delete the RL port.

Examples

Configure the ring RL port of ERPS ring 32 as ge1/1.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32rpl-portge1/1
Switch(config-erps-1)#
```

ring <1-32>revertive-behaviour

Command

```
ring <1-32>revertive-behaviour<non-revertive | revertive>
```

Mode

ERPS ring configuration mode

Parameters

None.

Description

The ring <1-32>revertive-behaviour command is to configure the recovery behavior of the ring, where non-revertive is non-recoverable and revertive is recoverable, and the default is recoverable.

Examples

Configure ERPS ring 32's to non-recoverable mode.

```
Switch(config)#erps 1
```

```
Switch(config-erps-1)#ring 32 revertive-behaviournon-revertive
Switch(config-erps-1)#
```

ring <1-32>guard-time

Command

```
ring <1-32>guard-time<time>
no ring <1-32>guard-time
```

Mode

ERPS ring configuration mode

Parameters

time: ring-guard-time time, in the range <10-2000>.

Description

The ring <1-32>guard-time command sets the guard-time of the ring, where the step is 10 millisecond, and the default is 500.

Examples

Configure the guard-time of ERPS ring 32 to 50.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 guard-time50
Switch(config-erps-1)#
```

ring <1-32>hold-off-time

Command

```
ring <1-32>hold-off-time<time>
no ring <1-32>hold-off-time
```

Mode

ERPS ring configuration mode

Parameters

time: ring hold-off time, range is <0-10000>.

Description

The ring <1-32>hold-off-time command sets the default value of ring hold-off time to 0 in steps of 100millisecond.

Examples

Configure the hold-off-time of ERPS ring 32 to 100.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 hold-off-time 100
Switch(config-erps-1)#
```

ring <1-32>wtr-time

Command

```
ring <1-32>wtr-time<time>
no ring <1-32>wtr-time
```

Mode

ERPS ring configuration mode

Parameters

time: the ring wtr-time time, in the range <1-12>.

Description

The ring <1-32> wtr-time command sets the default value of wtr-time for the ring to 5 minutes.

Examples

Configure ERPS ring 32 with a wtr-time of 1.

```
Switch(config)#erps 1
```

```
Switch(config-erps-1)#ring 32 wtr-time 1
Switch(config-erps-1)#
```

ring <1-32>wtb-time

Command

```
ring <1-32>wtb-time<time>
no ring <1-32>wtb-time
```

Mode

ERPS ring configuration mode

Parameters

time: the ring wtb-time time, in the range <1-10>.

Description

The ring <1-32> wtb-time command sets the default value of wtb-time for the ring to 5 seconds.

Examples

Configure ERPS ring 32 with a wtr-time of 1.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 wtr-time 1
Switch(config-erps-1)#
```

ring <1-32>raps-send-time

Command

```
ring <1-32>raps-send-time<time>
no ring <1-32>raps-send-time
```

Mode

ERPS ring configuration mode

Parameters

time: ring-raps-send-time time, in the range <1-10>.

Description

The ring <1-32>raps-send-time command is to set the ring protocol message sending time, the default value is 5 seconds.

Examples

Configure ERPS ring 32 to send protocol messages at 6.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 raps-send-time6
Switch(config-erps-1)#
```

ring <1-32>enable

Command

```
ring <1-32>enable
```

Mode

ERPS ring configuration mode

Parameters

None.

Description

The ring <1-32>enable command is to start the ring protocol.

Examples

Start ERPS Ring 32 protocol.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 enable
```

```
Switch(config-erps-1)#
```

ring <1-32>disable

Command

```
ring <1-32>disable
```

Mode

ERPS ring configuration mode

Parameters

None.

Description

The ring <1-32>disable command disables the ring protocol.

Examples

Start ERPS Ring 32 protocol.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 32 disable
Switch(config-erps-1)#
```

ring <1-32>forced-switch

Command

```
ring <1-32>forced-switch<if-name>
```

Mode

ERPS ring configuration mode

Parameters

if-name: port name, can be a physical port and a link aggregation port.

Description

The ring <1-32>forced-switch command forces the switch of the ERPS ring port.

Examples

Force switch ERPS ring port to ge1/1.

```
Switch(config)#erps 1
Switch(config-erps-1)# ring 32 forced-switch ge1/1
Switch(config-erps-1)#
```

ring <1-32>manual-switch

Command

```
ring <1-32>manual-switch<if-name>
```

Mode

ERPS ring configuration mode

Parameters

if-name: port name, can be a physical port and a link aggregation port.

Description

The ring <1-32>forced-switch command is to manually switch the ERPS ring port.

Examples

```
#Manually switch ERPS ring port to ge1/1.
Switch(config)#erps 1
Switch(config-erps-1)# ring 32 manual-switch ge1/1
Switch(config-erps-1)#
```

ring <1-32>clear

Command

```
ring <1-32>clear <forced-switch | manual-switch | recovery>
```

Mode

ERPS ring configuration mode

Parameters

None.

Description

The ring <1-32>clear command clears an ERPS ring from forced switching, manual switching, or manual recovery in case of unrecoverable behavior.

Examples

Clear forced switching of ERPS rings.

```
Switch(config)#erps 1
Switch(config-erps-1)# ring 32 clear forced-switch
Switch(config-erps-1)#
```

View command

show erps

Command

```
show erps [domain-id]
```

Mode

Normal mode / Privilege mode

Parameters

domain-id: ID number of the ERPS domain, in the range 1-8.

Description

The [no-domain-id] parameter displays the basic information of the currently configured erps ring.
Specify domain-id] to display the specifics of this erps ring.

Examples

```
Switch#show erps 8
domain 8 information
instance: 1
node role: interconnection
ring 1 information:
ring mode: major ring
node mode: ring node
rpl port: 2002
rl port: 2003
revertive behaviour: revertive
hold off time: 0s, 0ms
guard time: 0s, 500ms
wtr time: 5min
wtb time: 5s
raps send time: 5s
raps vlan: 2
traffic vlan list: vlan7 vlan6 vlan5 vlan4 vlan3 vlan1
enable state: enable
node state: idle
port list:
ring port: ge1/1, port mode: rpl port, port state: forwarding
```

```
ring port: ge1/2, port mode: rl port, port state: forwarding
```

Debugging commands

debug erps

Command

```
debug erps [all | events | packet [recv | send]]
no debug erps [all | events | packet [recv | send]]
```

Mode

Privilege mode

Parameters

all: Turn on all erps related debug switches.
events: Turn on the debug switch for erps event handling.
packet: Turn on the debug switch for erps protocol packets.
recv: Turn on the receive erps protocol messages debug switch only.
send: Turn on the debug switch for sending erps protocol messages only.

Description

The debug erps command is used to turn on the erps debug switch to enable users to see the erps event processing and protocol messages sent and received.
The no debug erps command is used to turn off the erps debug switch.

Examples

```
Turn on the debug switch for the erps protocol package at
Switch#debug erps packet
Switch#log display
```

CHAPTER 11

AAA command

802.1x commands

dot1x

Command

```
dot1x
no dot1x
```

Mode

Global configuration mode

Parameters

None

Description

The dot1x command opens the 802.1x protocol of the switch. To establish the AAA environment, you must first execute this command to open the 802.1x protocol.
The no dot1x command disables the 802.1x protocol on the switch. The AAA environment cannot be established after the 802.1x protocol is disabled.

Examples

Turn on the 802.1x protocol.

```
Switch#con t
Switch(config)#dot1x
Switch(config)#
#Disable 802.1x protocol.
Switch#con t
Switch(config)#no dot1x
Switch(config)#
```

dot1x default

Command

```
dot1x default
```

Mode

Global configuration mode

Parameters

None

Description

Return the 802.1x protocol configuration to the default state.

Examples

Bring the 802.1x protocol configuration back to the default state.

```
Switch# dot1x default
Switch#
```

dot1x control auto

Command

```
dot1x control auto { antiarp }
```

Mode

Interface configuration mode.

Parameters

Antiarp: Whether to enable dot1x ip-mac binding.

Description

Configure a port to be in auto state, and users under this port need to be authenticated before they can access the network.
When configured as antiarp, it means that the switch discards the packet when it receives a packet with a different ip mac address from the authenticated one.

Examples

```
#start port ge1/1 for dot1x ip-mac binding.
Switch(config-ge1/1)#dot1x control auto antiarp
Switch(config-ge1/1)#
```

dot1x control force-authorized

Command

```
dot1x control force-authorized
```

Mode

Interface configuration mode.

Parameters

None.

Description

Configure a port to be in the force-authorized state so that users under this port can access the network without authentication.

Examples

Configure port ge1/1 to be force-authorized.

```
Switch(config-ge1/1)#dot1x control force-authorized
Switch(config-ge1/1)#
```

dot1x control force-unauthorized

Command

```
dot1x control force-unauthorized
```

Mode

Interface configuration mode.

Parameters

None.

Description

Configure a port to be force-unauthorized so that users under this port can never access the network.

Examples

Configure port ge1/1 to force-unauthorized state.

```
Switch(config-ge1/1)#dot1x control force-unauthorized
Switch(config-ge1/1)#
```

no dot1x control

Command

```
no dot1x control
```

Mode

Interface configuration mode.

Parameters

None.

Description

Configure a port to N/A status, and users under this port can access the network without authentication.

Examples

Configure port ge1/1 for N/A status.

```
Switch(config-ge1/1)#no dot1x control
Switch(config-ge1/1)#
```

dot1x reauthenticate

Command

```
dot1x reauthenticate
no dot1x reauthenticate
```

Mode

Global configuration mode.

Parameters

None.

Description

dot1x reauthenticate turns on the re-authentication mechanism of the 802.1x protocol.
no dot1x reauthenticate disables the re-authentication mechanism of the 802.1x protocol.

Examples

Turn on the re-authentication mechanism.

```
Switch(config)#dot1x reauthenticate
Switch#
```

Disable the re-authentication mechanism.

```
Switch(config)#no dot1x reauthenticate
Switch#
```

dot1x timeout re-authperiod

Command

```
dot1x timeout re-authperiod <interval>
```

Mode

Global configuration mode.

Parameters

interval: Specifies the time interval in seconds for re-authentication.

Description

Configure the time interval for re-authentication of 802.1x protocol.

Examples

Configure the re-authentication interval to 1000 seconds.

```
Switch(config)#dot1x timeout re-authperiod 1000
Switch#
```

dot1x support-host

Command

```
dot1x support-host <number>
```

Mode

Interface configuration mode.

Parameters

number: The maximum number of authenticated hosts for the specified port.

Description

Configure the maximum number of authenticated hosts for the port.

Examples

Configure port ge1/1 to access a maximum number of hosts of 100.

```
Switch(config-ge1/1)#dot1x support-host 100
Switch(config-ge1/1)#
```

dot1x timeout tx-period

Command

```
dot1x timeout tx-period <interval>
```

Mode

Global configuration mode.

Parameters

interval: Specifies the interval, in seconds, for the switch to resend EAP-Request protocol packets.

Description

Configure the interval for the switch to resend EAP-Request protocol packets.

Examples

Configure the switch to resend EAP-Request protocol packets at an interval of 20 seconds.

```
Switch(config)#dot1x timeout tx-period 20
Switch(config)#
```

dot1x max-req

Command

```
dot1x max-req <number>
```

Mode

Global configuration mode.

Parameters

number: Specifies the number of times the switch will resend EAP-Request protocol packets.

Description

Configure the number of times the switch will resend EAP-Request protocol packets.

Examples

Configure the switch to retransmit EAP-Request protocol packets 2 times.

```
Switch(config)#dot1x max-req 2
Switch(config)#
```

dot1x timeout quiet-period

Command

```
dot1x timeout quiet-period <interval>
```

Mode
Global configuration mode.

Parameters
interval: Specifies the interval, in seconds, to wait for re-authentication when user authentication fails.

Description
Configure the interval to wait for re-authentication when user authentication fails.

Examples
Configure the interval to wait for re-authentication when user authentication fails to be 20 seconds.

```
Switch(config)#dot1x timeout quiet-period 20
Switch(config)#
```

dot1x timeout server-timeout

Command

```
dot1x timeout server-timeout <interval>
```

Mode
Global configuration mode.

Parameters
interval: Specifies the interval, in seconds, for the switch to resend RADIUS packets to the authentication server.

Description
Configure the interval between retransmissions of RADIUS packets from the switch to the authentication server.

Examples
Configure the switch to retransmit RADIUS packets to the authentication server at an interval of 20 seconds.

```
Switch(config)#dot1x timeout server-timeout 20
Switch(config)#
```

dot1x timeout supp-timeout

Command

```
dot1x timeout supp-timeout <interval>
```

Mode
Global configuration mode.

Parameters
interval: Specifies the interval in seconds between retransmissions of eap request packets from the switch to the client.

Description
Configure the interval between retransmissions of eap request packets from the switch to the client.

Examples
Configure the switch to retransmit eap request packets to the client at an interval of 30 seconds.

```
Switch(config)#dot1x timeout supp-timeout 30
Switch(config)#
```

dot1x transmit-port

Command

```
dot1x transmit-port
no dot1x transmit-port
```

Mode
Interface configuration mode.

Parameters
None.

Description
Configure the switch's port connecting the client and the authentication switch as a transport port to forward eapol authentication packets between the client and the 802.1x authentication switch.

Examples
Configure port ge1/1 as a transport port.
```
Switch(config-ge1/1)#dot1x transmit-port
Switch(config-ge1/1)#
```
Configure port ge1/1 as a non-transmission port.
```
Switch(config-ge1/1)#no dot1x transmit-port
Switch(config-ge1/1)#
```

dot1x client-version

Command
```
dot1x client-version <string>
```

Mode
Global configuration mode.

Parameters
string: Specify the version number of the 802.1x client.

Description
Configure the version number of the 802.1x client

Examples
Configure the version number of the 802.1x client as
```
Switch(config)# dot1x client-version 2.0
Switch(config)#
```

dot1x check-client

Command
```
dot1x check-client
```

Mode
Global configuration mode.

Parameters
None.

Description
The configuration checks if the client exists.

Examples
```
Switch(config)#dot1x check-client
Switch(config)#
```

dot1x check-version

Command
```
dot1x check-version {open | close }
```

Mode
Global configuration mode.

Parameters
open: Check the client version number.
close: Do not check the client version number.

Description
Configure whether to check the client version.

Examples
```
Switch(config)#dot1x check-client
Switch(config)#
```

show dot1x

Command
```
show dot1x
show dot1x interface
```

Mode
Privilege mode.

Parameters
None.

Description
When the command is show dot1x, it displays all 802.1x configuration information, including the configuration information of all ports; when the command is show dot1x interface, it displays the information of all access users under this port.

Examples
Display all 802.1x configuration information.
```
Switch#show dot1x
Switch#
```
Display information about all access users under the port.
```
Switch#show dot1x interface
Switch#
```

radius-server command

radius-server host

Command
```
radius-server host <ip-address>
```

Mode
Global configuration mode.

Parameters
ip-address: Specify the IP address of the primary authentication server.

Description
Configure the IP address of the primary authentication server.

Examples
Configure the primary authentication server as 198.168.80.111.
```
Switch(config)#radius-server host 198.168.80.111
Switch(config)#
```

radius-server option-host

Command
```
radius-server option-host <ip-address>
```

Mode
Global configuration mode.

Parameters
ip-address: Specify the IP address of the backup authentication server.

Description
Configure the IP address of the backup authentication server.

Examples
Configure the backup authentication server as 198.168.80.110.

```
Switch(config)#radius-server option-host 198.168.80.110
Switch(config)#
```

radius-server key

Command

```
radius-server key <string>.
```

Mode
Global configuration mode.

Parameters
string: Specifies the shared key of the switch.

Description
Configure the shared key for mutual authentication between the switch and the authentication server.

Examples
Configure the shared key of the switch as abcdef.

```
Switch(config)#radius-server key abcdef
Switch(config)#
```

radius-server accounting

Command

```
radius-server accounting
no radius-server accounting
```

Mode
Global configuration mode.

Parameters
None.

Description
radius-server accounting turns on the switch's billing function.
no radius-server accounting disables the switch's billing function.

Examples
Turn on the billing function.

```
Switch(config)#radius-server accounting
Switch(config)#
#Disable billing function.
Switch(config)#no radius-server accounting
Switch(config)#
```

radius-server udp-port

Command

```
radius-server udp-port <port-number>
```

Mode
Global configuration mode.

Parameters
port-number: Specifies the UDP port number of the authentication packet between the switch and the authentication server.

Description
Configure the UDP port number for authentication packets between the switch and the authentication server. Normally users do not need to modify the authentication UDP port number.

Examples
Configure the UDP port number for authentication packets to 1812.
```
Switch(config)#radius-server udp-port 1812
Switch(config)#
```

radius-server attribute nas-portnum

Command
```
radius-server attribute nas-portnum <number>
```

Mode
Global configuration mode.

Parameters
number: Specifies the value of the NASPort attribute.

Description
Configure the NASPort attribute value.

Examples
Configure the NASPort attribute with a value of 1000.
```
Switch(config)#radius-server attribute nas-portnum 1000
Switch(config)#
```

radius-server attribute nas-porttype

Command
```
radius-server attribute nas-porttype <number>
```

Mode
Global configuration mode.

Parameters
number: Specifies the value of the NASPortType attribute.

Description
Configure the NASPortType attribute value.

Examples
Configure the NASPortType attribute with a value of 10.
```
Switch(config)#radius-server attribute nas-porttype 10
Switch(config)#
```

radius-server attribute service-type

Command
```
radius-server attribute service-type <number>
```

Mode
Global configuration mode.

Parameters
number: Specifies the value of the NASPortServer attribute.

Description
Configure the NASPortServer attribute value.

Examples
Configure the NASPortServer attribute with a value of 3.
```
Switch(config)#radius-server attribute service-type 3
Switch(config)#
```

radius-server vsa

Command
```
radius-server vsa <string>
```

Mode
Global configuration mode.

Parameters
string: Specify vendor-specific information.

Description
Configure vendor-specific information in the RADIUS attribute.

Examples
Configure vendor-specific information as AAA.
```
Switch(config)# radius-server vsa AAA
Switch(config)#
```

radius-server roam

Command
```
adius-server roam
no radius-server roam
```

Mode
Global configuration mode.

Parameters
None.

Description
adius-server roam opens the RADIUS roaming feature.
no radius-server roam Disables the RADIUS roaming feature.

Examples
Configure RADIUS roaming function.
```
Switch(config)#radius-server roam
Switch(config)#
#Disable RADIUS roaming function.
Switch(config)#no radius-server roam
Switch(config)#
```

show radius-server

Command
```
show radius-server
```

Mode
Normal mode/privileged mode.

Parameters
None.

Description
Displays information related to RADIUS configuration.

Examples
Display RADIUS configuration information.
```
Switch#show radius-server
Switch#
```

Tacacs+ Commands

tacacsplus

Command
```
tacacsplus enable/ disable
```

Mode
Global configuration mode.

Parameters
enable/ disable: tacacs on and off.

Description
Enables/disables the TACACS+ function.

Examples
```
Switch(config)#tacacsplus enable
```

tacacsplus host

Command
```
tacacsplus host <server-ip>
```

Mode
Global configuration mode.

Parameters
server-ip: The IP address of the tacac+ server, supporting both ipv4 and ipv6 addresses.

Description
Configure the master server address.

Examples
```
Switch(config)#tacacsplus host 172.20.7.16
```

tacacsplus key

Command
```
tacacsplus key WORD
```

Mode
Global configuration mode.

Parameters
WORD: less than 30 characters.

Description
Configure the shared key.

Examples
```
Switch(config)#tacacsplus key 123456 ....
```

tacacsplus auth-type

Command

```
tacacsplus auth-type (PAP|CHAP)
```

Mode

Global configuration mode.

Parameters

PAP|CHAP: PAP/CHAP authentication method.

Description

Configure the authentication method.

Examples

```
Switch(config)#tacacsplus auth-type chap
```

tacacsplus option-host

Command

```
tacacsplus option-host<server-ip>
```

Mode

Global configuration mode.

Parameters

server-ip: The IP address of the alternate tacac+ server, supporting both ipv4 and ipv6 addresses.

Description

Configure the standby server address.

Examples

```
Switch(config)#tacacsplus option-host 172.20.7.17
```

show tacacsplus

Command

```
Show tacacsplus
```

Mode

Privilege mode.

Parameters

None.

Description

View TACACS+ configuration information.

Examples

```
Switch#show tacacsplus
Tacacs+ Protocol : Disable
Tacacs+ Authentication Type : PAP
Tacacs+ Host : 3FFE:507::1:4000:0:0:253
Tacacs+ Option-host : 198.168.88.253
Tacacs+ Shared Secret : cisco
Switch#...
```

CHAPTER 12

GMRP command

GMRP configuration commands

set gmrp

Command

```
Set gmrp { enable | disble }
```

Mode

Global configuration mode

Parameters

None.

Description

set gmrp enable Enables global all vlan gmrp
set gmrp disable to enable global all vlan gmrp

Examples

```
#start global gmrp protocol
Switch#configure terminal
Switch(config)#set gmrp enable
Switch(config)#
```

set gmrp enable vlan

Command

```
set gmrp {enable |disble} vlan<vlan-id>
```

Mode

Global configuration mode

Parameters

vlan-id: vlan number, range 1-4094.

Description

set gmrp enable vlan enable global specific vlan gmrp
set gmrp disable vlan to enable global specific vlan gmrp

Examples

start gmrp protocol for vlan1

```
Switch#configure terminal
Switch(config)#set gmrp enable vlan 1
Switch(config)#
```

set gmrp registration

Command

```
set gmrp registration{fixed | forbidden | normal} <if-name>
```

Mode

Global configuration mode

Parameters

if-name: Interface number.

Description
set gmrp registration configure interface registration multicast mode

Examples
Set the registered multicast mode of port ge1/1 to fixed.

```
Switch#configure terminal
Switch(config)#set gmrp registration fixed ge1/1
Switch(config)#
```

set gmrp timer

Command

```
set gmrp timer {join | leave | leaveall} <time-value>
```

Mode
Global configuration mode

Parameters
time-value: time.

Description
set gmrp timer to configure the time of various timers

Examples
Set the time of leaveall to 2000 centiseconds.

```
Switch#configure terminal
Switch(config)#set gmrp timer leaveall 2000 ge1/1
Switch(config)#
```

set port gmrp

Command

```
set port gmrp {enable |disable} <if-name>
```

Mode
Global configuration mode

Parameters
if-name: Port number.

Description
set port gmrp {enable |disable} {enable|de-enable} port GMRP function

Examples

```
#Enable port ge1/1 GMRP function.
Switch#configure terminal
Switch(config)#set port gmrp enable ge1/1
Switch(config)#
```

GMRP display command

show gmrp configuration

Command

```
show gmrp configuration
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
show gmrp configuration View GMRP configuration information

Examples

```
Switch#show gmrp configuration
Global GMRP Configuration for bridge :1
GMRP Feature: Enabled
Port based GMRP Configuration:
Timers(centiseconds)
Port GMRP Status Registration Forward All Join Leave LeaveAll
------------------------------------------------------------------------------
ge1/2 Enabled Normal Disabled 20 60 1000
Switch#
```

show gmrp machine

Command

```
show gmrp machine
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
show gmrp machine to view GMRP status machine information

Examples

```
Switch#show gmrp machine
Port VLAN MAC Address StateRegistrarStateApplicant
------ ---- -------------- --------------- ---------------
ge1/2 20 0100.5e01.0101 MTQA
Switch#
```

show gmrp statistics vlanid

Command

```
show gmrp statistics vlanid
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
show gmrp statistics vlanid View gmrp statistics for a specific vlanid

Examples

```
Switch#show gmrp statistics vlanid 1
GMRP Statistics for bridge 1 vlan 1
-------------------------------------------------
Total GMRP packets Received: 0
Leave alls: 0
Join Empties: 0
Join Ins: 0
Leave Empties: 0
Leave Ins: 0
Empties: 0
Total GMRP packets Transmitted: 0
Leave alls: 0
```

```
Join Empties: 0
Join Ins: 0
Leave Empties: 0
Leave Ins: 0
Empties: 0
Switch#
```

show gmrp timer

Command

```
show gmrp timer<if-name>
```

Mode

Normal mode / Privilege mode

Parameters

if-name: Interface number.

Description

show gmrp timer to see the timer information for a specific port

Examples

```
Switch#show gmrp timer ge1/3
Timer Timer Value (centiseconds)
----------------------------------------
Join 20
Leave 60
Leave All 1000
Switch#
```

GMRP debugging commands

debug gmrp

Command

```
[no] debug gmrp {all |cli| event| packet|timer}
```

Mode

Privilege mode

Parameters

None.

Description

The debug gmrp command is used to open GMRP debugging information.

Examples

Open all debug information of gmrp.

```
Switch#debug gmrp all
Switch#
```

debug garp

Command

```
[no] debug garp {all |cli| event| packet|timer}
```

Mode

Privilege mode

Parameters

None.

Description

The debug garp command is used to open GARP debugging information.

Examples

```
#Open all debug information of garp.
Switch#debug garp all
Switch#
```

show debugging gmrp

Command

```
show debugging gmrp
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

show debugging gmrp is used to see which GMRP debug switches are enabled

Examples

```
Switch#show debugging gmrp
GMRP debugging status:
GMRP event debugging is on
GMRP timer debugging is on
GMRP packet debugging is on
GMRP cli debugging is on
Switch#
```

CHAPTER 13

IGMP SNOOPING command

IGMP SNOOPING configuration command

ip igmp snooping

Command

```
ip igmp snooping
no ip igmp snooping
```

Mode

Global configuration mode

Parameters

None

Description

The ip igmp snooping command is used to start the igmp snooping function for all vlan.
The no ip igmp snooping command disables the igmp snooping function for all vlan.

Examples

```
None.
```

ip igmp snooping fast-leave

Command

```
ip igmp snooping fast-leave vlan <vlan-id>
no ip igmp snooping fast-leave vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

vlan-id: The vlan number to start the immediate departure.

Description

Start the IGMP V2 immediate leave feature for a vlan.
The no command disables the IGMP V2 immediate leave feature for a vlan.

Examples

Start multicast members of vlan2 to immediately leave the function.

```
Switch(config)#ip igmp snooping fast-leave vlan 2
Switch(config)#
```

ip igmp snooping fast-leave-timeout

Command

```
ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>
no ip igmp snooping fast-leave-timeout vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

interval: delay time, in ms, unlimited range. The default is 300000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description

Set the multicast member of a vlan to leave the delay time immediately and wait for the time specified in the interval before removing the member after receiving the leave packet.
The no command cancels the immediate leave delay setting, and the interval restores the default value.

Examples

Configure vlan1 to delete a multicast member as soon as it receives a leave packet from that member.

```
Switch(config)#ip igmp snooping fast-leave vlan 1
Switch(config)#ip igmp snooping fast-leave-timeout 0 vlan 1
Switch(config)#
```

ip igmp snooping group-membership-timeout

Command

```
ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
no ip igmp snooping group-membership-timeout vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

interval: member survival time, in ms, range is unlimited. The default is 400000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description

Configure the survival time of multicast groups that join after receiving a REPORT packet.
The no command cancels the configuration of member survival time and restores the default value.

Examples

Configure vlan2 with a multicast membership survival time of 600 seconds.

```
Switch(config)#ip igmp snooping group-membership-timeout 600000 vlan 2
Switch(config)#
```

ip igmp snooping mrouter

Command

```
ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]
no ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]
```

Mode

Global configuration mode

Parameters

if-name: The name of the interface.
vlan-id: The vlan number to which the interface belongs.

Description

Configure the query port to which all other ports will forward any multicast join-leave packets they receive; the port will join the multicast group.
The no command removes the configured query port.

Examples

Configure port ge1/1 as a query port for vlan2.

```
Switch(config)#ip igmp snooping mrouter interface ge1/1 vlan 2
Switch(config)#
```

ip igmp snooping query-membership-timeout

Command

```
ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
no ip igmp snooping query-membership-timeout vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
interval: the survival time of the query port, in ms, range 60000-300000ms. default 300000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description
Configure the survival time of the query group joined after receiving a QUERY packet.
The no command cancels the configuration of the query group survival time and restores the default value.

Examples
Configure vlan2 to query the port for 600 seconds.

```
Switch(config)#ip igmp snooping query-membership-timeout 600000 vlan 2
Switch(config)#
```

ip igmp snooping vlan

Command

```
ip igmp snooping vlan <vlan-id>
no ip igmp snooping vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
vlan-id: vlan number.

Description
To start the igmp snooping function of a vlan, you must execute ip igmp snooping before you can configure the igmpsnoop function of a vlan.
The no command disables the igmp snooping function for a vlan.

Examples
Turn off igmp snooping for vlan3 and turn on igmp snooping for other vlan.

```
Switch(config)#no ip igmp snooping vl
Switch(config)#no ip igmp snooping vlan 3
Switch(config)#
```

ip igmp snooping querier vlan

Command

```
ip igmp snooping querier vlan <vlan-id>
no ip igmp snooping querier vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
vlan-id: vlan number.

Description
Start the igmp snooping query function for a vlan.
The no command disables the igmp snooping query function for a vlan.

Examples
Turn on the igmp snooping query function for vlan1.

```
Switch(config)#ip igmp snooping querier vlan 1
```

Disable the igmp snooping query function for vlan1.

```
Switch(config)#no ip igmp snooping querier vlan 1
```

ip igmp snooping send-query version

Command

```
ip igmp snooping send-query version<v1 | v2 | v3>
```

Mode

Global configuration mode

Parameters

v1 | v2 | v3: Version number.

Description

Set the version number for sending igmp snooping query packets.

Examples

Set the version for sending igmp snooping query packets to v2.

```
Switch(config)#ip igmp snooping send-query version v2
```

ip igmp snooping send-query source-address

Command

```
ip igmp snooping send-query source-address<source-ip>
```

Mode

Global configuration mode

Parameters

source-ip: source IP.

Description

Set the source IP address for sending igmp snooping query packets.

Examples

Set the source IP address for sending igmp snooping query packets to 192.168.0.100.

```
Switch(config)#ip igmp snooping send-query source-address 192.168.0.100
Switch(config)#
```

ip igmp snooping query-interval

Command

```
ip igmp snooping query-interval<interval> vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

interval: the time interval for sending query packets, the range is 60000-125000, unit: ms
vlan-id: vlan number

Description

Set the time interval for sending igmp snooping query packets.

Examples

Set the time interval for vlan 2 to send igmp snooping query packets to 60000ms.

```
Switch(config)#ip igmp snooping query-interval 60000 vlan 2
Switch(config)#
```

ip igmp snooping filter-rule

Command

```
ip igmp snooping filter-rule<rule-id><permit | deny><min-ipaddress> [max-ipaddress]
no ip igmp snooping filter-rule<rule-id>
```

Mode
Global configuration mode

Parameters
rule-id: rule id, range 1-100.
min-ipaddress: Multicast address
max-ipaddress: multicast address, must be greater than the min-ipaddress address

Description
The ip igmp snooping filter-rule command is used to configure the igmp snooping multicast filtering rule function.
The noip igmp snooping filter-rule command is used to delete a multicast filtering rule.

Examples
Configure a multicast filter rule of 1 and do not allow multicast 234.0.0.1 addresses to pass

```
Switch#configure terminal
Switch(config)#ip igmp snooping filter-rule 1 deny 234.0.0.1
Switch(config)#
```

ip igmp snooping filter-group

Command

```
ip igmp snooping filter-group<rule-id>
no ip igmp snooping filter-group
```

Mode
Interface configuration mode

Parameters
rule-id: rule id, range 1-100.

Description
The ip igmp snooping filter-group command is used to configure a port to refer to a group of multicast filtering rules.
The noip igmp snooping filter-group command is used to remove the multicast filtering referenced by the port.

Examples
Delete the multicast filtering rule for port ge1/1.

```
Switch#configure terminal
Switch(config)#int ge1/1
Switch(config-ge1/1)#no ip igmp snooping filter-group
Switch(config-ge1/1)#
```

IGMP SNOOPING view command

show ip igmp snooping

Command

```
show ip igmp snooping [fast-leave [vlan <vlan-id>] | fast-leave-timeout [vlan <vlan-id>] |
forwarding-table | group-membership- timeout [vlan <vlan-id>] | interface [vlan <vlan-id>] |
query-membership-timeout [vlan <vlan-id>] | vlan <vlan-id> ]
```

Mode
Normal mode / Privilege mode

Parameters
fast-leave: Displays the opening of the leave-now feature.
vlan <vlan-id>: Displays the configuration of the specified vlan.
fast-leave-timeout: Displays the configuration of the immediate leave delay time.

forwarding-table: Displays the multicast forwarding table, including the multicast group and corresponding vlan and port.
group-membership-timeout: Displays the group membership survival time configuration.
interface: Shows the relationship between the available ports and vlan.
query-membership-timeout: Displays the query group survival time configuration.
vlan: Displays the igmp snooping configuration for the specified vlan.

Description
Display the igmp snooping configuration.

Examples
Display the igmp snooping configuration for vlan1.

```
Switch#show ip igmp snooping vlan 1
Bridge 1 VLAN 0:
IGMP Snooping is globally enabled
Bridge 1: VLAN 1
IGMP Snooping is enabled
IGMP Snooping fast-leave is enabled
IGMP Snooping fast-leave-timeout is 300000 ms
IGMP snooping query membership timeout is 300000 ms
IGMP snooping group membership timeout is 400000 ms
Switch#
```

show ip igmp snooping age-table

Command

```
show ip igmp snooping age-table { group-membership | query-membership}
```

Mode
Normal mode / Privilege mode

Parameters
group-membership: Displays the age time of the member group.
query-membership: Display the age time of the query group.

Description
Displays the age time and the port where the multicast group is located.

Examples

```
#Display the age time of the member group.
Switch#show ip igmp snooping age-table group-membership
VLAN Address Port Seconds
3 239.255.255.250 ge1/1 340000 ms
Switch#
```

show ip igmp snooping mrouter

Command

```
show ip igmp snooping mrouter [interface <if-name> | vlan <vlan-id>]
```

Mode
Normal mode / Privilege mode

Parameters
interface <if-name>: Displays the ability of the specified port to
vlan <vlan-id>: Displays the query port of the specified vlan.

Description
Displays the query port information.

Examples
Show query ports for vlan3.

```
Switch#show ip igmp snooping mrouter vlan 3
Bridge VLAN Ports
--------------- ----- -----------------
1 3 ge1/1,
Switch#
```

show ip igmpv2

Command

```
show ip igmpv2 snooping statistics [vlan <vlan-id>]
```

Mode

Normal mode / Privilege mode

Parameters

vlan <vlan-id>: Displays the status of the specified vlan.

Description

Displays statistics for igmpv2 protocol packets.

Examples

Display igmpv2 protocol packet statistics for vlan1.

```
Switch#show ip igmpv2 snooping statistics vlan 1
IGMP-V2 Snooping Statistics: Bridge 1 VLAN default
Total valid pkts rcvd : 0
Total invalid pkts rcvd : 0
Number of Reports rcvd : 0
Number of Leaves rcvd : 0
Number of Membership Queries rcvd : 0
Number of Reports tx : 0
Number of Leaves tx : 0
Number of Group-Specific Queries tx : 0
Number of General Queries tx : 0
Switch#
```

show ip igmp snooping explicit-tracking

Command

```
show ip igmp snooping explicit-tracking vlan <vlan-id>
```

Mode

Normal mode / Privilege mode

Parameters

vlan-id: vlan number.

Description

Displays the status and details of the igmp snooping explicit-tracking feature for a vlan.

Examples

```
#Show igmp snooping explicit-tracking function for vlan1
Switch#show ip igmp snooping explicit-tracking vlan 1
Switch#
```

show ip igmp snooping ssm-safe-reporting

Command

```
show ip igmp snooping ssm-safe-reporting vlan <vlan-id>
```

Mode

Normal mode / Privilege mode

Parameters
vlan-id: vlan number.

Description
Displays the status of the igmp snooping ssm-safe-reporting function for the relevant vlan.

Examples
```
#Show the status of igmp snooping ssm-safe-reporting function of vlan1
Switch#show ip igmp snooping ssm-safe-reporting vlan 1
```

show ip igmpv3

Command
```
show ip igmpv3 snooping statistics [vlan <vlan-id>]
```

Mode
Normal mode / Privilege mode

Parameters
vlan <vlan-id>: Displays the status of the specified vlan.

Description
Displays statistics for igmpv3 protocol packets.

Examples
show igmpv3 protocol packet statistics for vlan1.
```
Switch#show ip igmpv3 snooping statistics vlan 1
```

IGMP SNOOPING debugging command

debug igmp snooping

Command
```
debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]
no debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]
```

Mode
Privilege mode.

Parameters
all: Turn on all debug switches for igmp snooping.
cli: cli command prompt.
events: Turn on the igmp snooping time debugging switch.
packet: Turn on the igmp snooping packet debugging switch.
timer: Turn on the igmp snooping timer debug switch.

Description
The debug igmp snooping command is used to turn on the igmp snooping-related debug switch to enable users to see the events and messages sent and received related to igmp snooping.
The no debug igmp snooping command disables the corresponding igmp snooping debug switch.

Examples
Turn on the igmp snooping message debugging switch.
```
Switch#debug igmp snooping packet
Switch#
```

CHAPTER 14

MVR command

MVR configuration commands

mvr enable

Command

```
mvr {enable|disable}
```

Mode

Global configuration mode

Parameters

None

Description

The mvr enable|disable command is used to enable and disable the mvr function.

Examples

```
#Start mvr protocol
Switch#configure terminal
Switch(config)#mvr enable
Switch(config)#
```

no mvr

Command

```
no mvr
```

Mode

Global configuration mode

Parameters

None

Description

The no mvr command is used to clear all MVR configurations

Examples

Clear all MVR configurations

```
Switch#configure terminal
Switch(config)#no mvr
Switch(config)#
```

mvr group

Command

```
mvr group <multicast-address>
mvr group <multicast-address><num>
no mvr group <multicast-address>
```

Mode

Global configuration mode

Parameters

<multicast-address>:Multicast address

num: consecutive addresses, range <1-256>

Description
mvr group <multicast-address>: Configure IP multicast address
no mvr group <multicast-address>: Delete the IP multicast address

Examples
```
Switch(config)#mvr group 225.0.0.1
```

mvr vlan

Command
```
mvr vlan <vlanid>
no mvr vlan
```

Mode
Global configuration mode

Parameters
vlanid: specific vlan, range <1-4094>

Description
mvr vlan <1-4094>: Configure the VLAN that is specified to receive multicast data
no mvr vlan: Restore the default VLAN1 for receiving multicast data

Examples
```
Switch(config)#mvr vlan 2
```

mvr-interface

Command
```
mvr-interface enable|disable
```

Mode
Interface configuration mode

Parameters
None

Description
mvr-interface enable|disable: enables and disables the interface MVR

Examples
```
Switch(config-ge1/1)#mvr-interface enable
```

View command

show mvr

Command
```
show mvr
```

Mode
Normal mode / Privilege mode

Parameters
None

Description
show mvr: Display MVR configuration information

Examples
```
Switch#show mvr
mvr running : disable
```

```
mvr multicast vlan : 1
mvr group ip (total have 0 group ip address) :
mvr related interface (total have 0 interface) :
Switch#
```

CHAPTER 15

DHCP SNOOPING

dhcp snooping configuration command

ip dhcp snooping

Command

```
ip dhcp snooping [IF_LIST]
no ip dhcp snooping
```

Mode

Global configuration mode.

Parameters

IF_LIST configures the list of physical ports that can be trusted to link DHCP server addresses, supporting up to 4 trusted ports.

Description

The ip dhcp snooping command starts the global dhcp snooping function.
no ip dhcp snooping Cancels the global dhcp snooping feature.

Examples

Configure the switch to start DHCP Snooping function and only the DHCP server connected to port ge1/5 is legitimate

```
Switch(config)#ip dhcp snooping ge1/5
Switch(config)#
```

dhcp snooping

Command

```
dhcp snooping
no dhcp snooping
```

Mode

Interface configuration mode.

Parameters

None.

Description

The dhcp snooping command indicates that the interface starts the dhcp snooping function.

Examples

```
#start dhcp snooping on port ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#
```

dhcp snooping option82

Command

```
dhcp snooping option82
no dhcp snooping option82
```

Mode

Interface configuration mode.

Parameters
None.

Description
The dhcp snooping option82 command indicates that the interface starts the dhcp snooping option82 function.

Examples
```
#start dhcp snooping option82 on port ge1/1
Switch(config-ge1/1)#dhcp snooping option82
Switch(config-ge1/1)#
```

dhcp snooping option82 circuit-id

Command
```
dhcp snooping option82 circuit-id<circuit-id>
no dhcp snooping option82 circuit-id
```

Mode
Interface configuration mode.

Parameters
circuit-id. circuit-id string, maximum length is 64 bits.

Description
The dhcp snooping option82 circuit-id command indicates to configure the circuit-id value of option82.

Examples
Configure the circuit-id of port ge1/1 option82 to abcde
```
Switch(config-ge1/1)#dhcp snooping option82 circuit-id abcde
Switch(config-ge1/1)#
```

dhcp snooping delete

Command
```
dhcp snooping delete <mac>
```

Mode
Global configuration mode.

Parameters
mac: mac address of the table entry to be deleted

Description
Manually delete a dhcp snooping table entry.

Examples
Delete the dhcp snooping table entry for 0009.ca01.0001.
```
Switch(config)#dhcp snooping delete 0009.ca01.0001
Switch(config)#
```

dhcp snooping view command

show dhcp snooping

Command
```
show dhcp snooping
```

Mode
Normal mode / Privilege mode.

Parameters
None.

Description
The show dhcp snooping command views dhcp snooping configuration information.

Examples
```
Switch#show dhcp snooping
DHCP Snooping is enabled globally
Enable interface: ge1/1
```

show dhcp snooping binding-table

Command
```
show dhcp snooping binding-table
```

Mode
Normal mode/privileged mode.

Parameters
None.

Description
The show dhcp snooping binding-table command views the information of the binding table learned by dhcp snooping.

Examples
```
Switch#show dhcp snooping binding-table
IP MAC FLAG PORT LEASE
00:40:05:11:69:60 ACK ge1/4 7D 22:11:44
```

dhcp snooping debug command

d ebug dhcp snooping

Command
```
debug dhcp snooping [all] | [events] | [packet]
no debug dhcp snooping [all] | [events] | [packet]
```

Mode
Privilege mode.

Parameters
all: Turn on all debug switches of dhcp.
events: Turn on the dhcp event debug switch.
packet: Turn on the dhcp message debug switch.

Description
The debug dhcp snooping command is used to turn on the dhcp-related debugging switch to enable users to see the dhcp-related events and messages sent and received.
The no debug dhcp snooping command disables the corresponding dhcp debug switch.

Examples
Turn on the dhcp message debugging switch.
```
Switch#debug dhcp snooping packet
Switch#
```

show debuggingdhcp snooping

Command
```
show debuggingdhcp snooping
```

Mode
Normal mode / Privilege mode

Parameters

None.

Description

The show debuggingdhcp snooping command is used to display the status of dhcp-related debugging switches.

Examples

Display dhcp message debug switch status.

```
Switch#show debugging dhcp snooping
DHCP Snooping debugging status:
DHCP Snooping packet receive debugging is on
DHCP Snooping packet send debugging is on
DHCP Snooping event debugging is on
```

CHAPTER 16

DHCP client command

dhcp client configuration commands

dhcp client enable

Command

```
dhcp client enable
no dhcp client enable
```

Mode

vlanif configuration mode.

Parameters

None.

Description

The dhcp client enable command enables the dhcp client function to obtain the interface address. no dhcp client enable cancels the dhcp client function.

Examples

```
#start the dhcp client function of vlan1
Switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client enable
```

dhcp client renew

Command

```
dhcp client renew
```

Mode

vlanif configuration mode.

Parameters

None.

Description

The dhcp client renew command reacquires the IP address for the interface.

Examples

```
#re-obtain IP address for interface vlan1
Switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client renew
```

dhcp client release

Command

```
dhcp client release
```

Mode

vlanif configuration mode.

Parameters

None.

Description
The dhcp client release command releases the interface IP address.

Examples
```
#release the IP address of interface vlan1
Switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client release
```

View command

show dhcp client

Command
```
show dhcp client
```

Mode
Privilege mode / Normal mode.

Parameters
None

Description
The show dhcp client command is used to view the information of the current dhcp client.

Examples
View information about the dhcp client.
```
Switch#show dhcp client
Interface vlan2
DHCP Client: Enabled
State: BOUND
IP Address: 2.0.0.1
Subnet Mask: 255.255.255.0
Default Gateway: 2.0.0.11
DHCP Server: 2.0.0.11
Lease Time: 691200(s)
Lease Expires: After 7 days 23 hours 55 minutes 49 seconds
```

CHAPTER 17

DHCP RELAY

dhcp relay configuration command

dhcp relay

Command

```
dhcp relay<ip-address-1> [ip-address-2]
no dhcp relay
```

Mode

Interface configuration mode.

Parameters

ip-address-1: The IP address of server 1, in 32-bit dotted decimal format.
ip-address-2: IP address of server 2, 32-bit dotted decimal format

Description

The dhcp relay command is used to enable the dhcp-relay function of the interface. The default does not enable the dhcp-relay function of the interface.
The no dhcp relay command is used to disable the dhcp-relay function of the interface.

Examples

```
#Enable the dhcp-relay function on interface vlan10.
Switch(config-vlan10)#dhcp relay 192.168.0.200
Switch(config-vlan10)#
```

View command

show dhcp relay

Command

```
show dhcp relay
```

Mode

Privilege mode / Normal mode.

Parameters

None

Description

The show dhcp relay command is used to view the information of the current dhcp relay configuration.

Examples

View information about the dhcp relay configuration.

```
Switch#show dhcp relay
Interface vlan1
DHCP Relay: Enabled
Server IP: 192.168.0.221
Switch#
```

CHAPTER 18

DHCP SERVER

dhcp server configuration commands

ip dhcp server

Command

```
ip dhcp server
no ip dhcp server
```

Mode

Global configuration mode

Parameters

None.

Description

The ip dhcp server command is to start the global DHCP SERVER function.
The no ip dhcp server command is to disable the global DHCP SERVER function.

Examples

Start global DHCP SERVER function

```
Switch(config)#ip dhcp server
#Disable global DHCP SERVER function
Switch(config)#no ip dhcp server
```

dhcp serverlisten

Command

```
dhcp serverlisten
no dhcp serverlisten
```

Mode

Interface configuration mode

Parameters

None.

Description

The dhcp serverlisten command is to start the interface dhcp server listening function.
The no dhcp serverlisten command disables the interface dhcp server listening function.

Examples

Start the dhcp server listening function on interface vlan1.

```
Switch(config-vlan1)#dhcp serverlisten
#Disable the dhcp server listening function on interface vlan1
Switch(config-vlan1)#no dhcp serverlisten
```

dhcp serverpool

Command

```
dhcp serverpool<pool-name>
no dhcp serverpool<pool-name>
```

Mode
Global configuration mode

Parameters
pool-name: The name of the address pool.

Description
The dhcp serverpool command is to establish address pool and enter address pool configuration mode.
The no dhcp serverpool command is to delete the address pool

Examples
```
#Enter the address pool named pool1
Switch(config)#dhcp serverpool pool1
#delete address pool named pool1 address pool
Switch(config)#no dhcp serverpool pool1
```

range

Command
```
range <low-address><high-address>
no range
```

Mode
Address pool configuration mode

Parameters
low-address: starting address
high-address:End address.

Description
range Configures the address range of the address pool.
no range Deletes the address range of the address pool.

Examples
Configure address pool1 range 192.168.0.2 192.168.0.100
```
Switch(config)#dhcp serverpool pool1
Switch(config-dhcp)#range 192.168.0.2 192.168.0.100
```
Delete the address range of address pool1
```
Switch(config-dhcp)#no range
```

lease

Command
```
lease { infinite | <day><hours><minutes>}
```

Mode
Address pool configuration mode

Parameters
day: number of days, range 0-999 days.
hours:Hours, range 0-23 hours.
minutes:minutes, range 0-59 minutes.

Description
The lease command is to configure the lease time of the address pool, the default is 8 days.

Examples
Configure address pool pool1 with a lease time of 9 days 9 hours and 9 minutes
```
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)#lease 9 9 9 9
```

default-router

Command

```
default-router<address>
no default-router
```

Mode

Address pool configuration mode

Parameters

address: The range of values is 0.0.0.0 to 223.255.255.255.

Description

The default-router command is to configure the default gateway for the address.
The no default-router command is to delete the default gateway for the address.

Examples

Configure the default gateway of address pool1 to 192.168.0.10

```
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)# default-router 192.168.0.10
```

subnet-mask

Command

```
subnet-mask<mask>
```

Mode

Address pool configuration mode

Parameters

mask: mask of the IP address, in dotted decimal format.

Description

The subnet-mask command is to configure the subnet mask of the address.

Examples

```
#Configure the subnet mask of address pool1 to 255.255.255.0
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)#subnet-mask 255.255.255.0
```

dns-server

Command

```
dns-server {<address1> [address2]}
no dns-server
```

Mode

Address pool configuration mode

Parameters

address1: The first DNS address, with a value range of 0.0.0.0 to 223.255.255.255.
address2: the second DNS address, the value range is: 0.0.0.0 ~ 223.255.255.255

Description

The dns-server command is to configure and modify the dns address of the address pool, up to two.
The no dns-server command is to delete the dns address of the address pool.

Examples

Configure the dns server of address pool1 as 210.21.223.113 and 210.22.223.11

```
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)#dns-server 210.21.223.113 210.22.223.11
```

exclude-address

Command

```
exclude-address<low-address>[high-address]
no exclude-address { all | <address> }
```

Mode

Address pool configuration mode

Parameters

low-address:Start exclude address.
high-address:End exclusion address.
address:The IP address to be excluded.
all:All excluded addresses.

Description

The exclude-address command is to configure the excluded addresses of the address pool.
The no exclude-address command is to delete the specified excluded address or all excluded addresses in the address pool.

Examples

Configure the excluded address 192.168.0.20 for address pool1

```
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)#exclude-address 192.168.0.20
#Configure the excluded address range of address pool2 from 192.168.2.20 to 192.168.2.30
Switch(config)#dhcp server pool pool2
Switch(config-dhcp)#exclude-address 192.168.2.20192.168.2.30
```

option82 circuit-id

Command

```
option82 circuit-id<circuit-id>
no option82circuit-id
```

Mode

Interface configuration mode.

Parameters

circuit-id. circuit-id string, maximum length is 64 bits.

Description

The option82 circuit-id command indicates the circuit-id value of option82 for the configured address pool.

Examples

Configure abcd of circuit-id of option82 of address pool1

```
Switch#con t
Switch(config)#dhcp server pool pool1
Switch(config-dhcp)#option82 circuit-id abcd
Switch(config-dhcp)#
```

View command

show dhcp server

Command

```
show dhcp server
```

Mode

Privilege mode / Normal mode.

Parameters
None

Description
The show dhcp server command is used to view the information of the current dhcp server configuration.

Examples
View information about the configuration of the dhcp server.

```
Switch#show dhcp server
DHCP server: Disable
DHCP server listen interface:
Switch#
Switch#
```

show dhcp server pool

Command

```
show dhcp server pool [pool-name]
```

Mode
Privilege mode / Normal mode.

Parameters
None

Description
The show dhcp server pool command is used to view the address pool configuration information.

Examples
View configuration information for address pool pool1.

```
Switch#show dhcp server pool pool1
Pool Name: pool1
Option 82: Enable
Option 82 Circuit String: abcd
Start IP: 192.168.0.100
End IP: 192.168.0.200
Subnet Mask: 255.255.255.0
Default Router: 192.168.0.1
DNS server: 114.114.114.14
Lease Time: 8 days 0 Hours 0 Minutes
Switch#
```

show dhcp serveraddress

Command

```
show dhcpserveraddres
```

Mode
Privilege mode / Normal mode.

Parameters
None.

Description
The show dhcp serveraddres command is used to view the table of assigned address information.

Examples
View dhcp server assigned address information.

```
Switch#show dhcp server address
IP MAC State Pool Name Lease
Switch#
```

Clear command

clear dhcp server address

Command

```
clear dhcp serveraddress{ <address> | all | }
```

Mode

Privilege mode.

Parameters

address:The specified IP address, expressed in 32-bit decimal
all contains all addresses.

Description

The clear dhcp server address command is used to clear the assigned address.

Examples

Clear the assigned address information.

```
Switch#clear dhcp server address
Switch#
```

clear dhcp serveraddress conflict

Command

```
clear dhcp server addressconflict{ <address> | all | }
```

Mode

Privilege mode.

Parameters

address:The specified IP address, expressed in 32-bit decimal
all contains all addresses.

Description

The clear dhcp server addressconflict command is used to clear conflicted addresses.

Examples

Clear conflicted address information.

```
Switch#clear dhcp server addressconflict
Switch#
```

CHAPTER 19

ACL commands

ACL configuration commands

Standard ACL rules

Command

```
access-list {<group-id>} {permit | deny | remark} {<source-ip>}
```

Mode

Global configuration mode

Parameters

group-id: rule group number, range: <1-99>|<1300-1999>.
permit: Allow packets that match the rule to be forwarded.
deny: Prohibit packets that match the rule from being forwarded.
remark: adds a comment to the specified rule group.
source-ip: source IP, with three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
wildcard: The reverse mask, which determines which bits need to be matched, '0' means they need to be matched, '1' means they don't need to be matched.

Description

Configure standard IP-based ACL access control rules. This type of rule only determines whether the source IP address of the packet matches the configured ACL rule; if it matches, it is processed accordingly according to deny/permit. In all ACL rules there is a deny all IP packets hidden rule, as long as the user has configured an ACL rule, the system will automatically generate this rule. Therefore, the user does not need to manually deny any of the configuration. The same is true for extended IP-based rules and MAC address-based rules.

Examples

Configure a set of rules that allow packets with source address 192.168.0.0 segment to be forwarded and prohibit packets with source address 192.168.0.11 and other addresses to be forwarded.

```
Switch(config)#access-list 1 deny host 192.168.0.11
Switch(config)#access-list 1 permit 192.168.0.0 0.0.0.255
Switch(config)#access-list 1 deny any
```

Extended ACL rules

Command

```
access-list {<group-id>} {permit | deny | remark} {protocol} {<source-ip>} [<source-port>]
{<dest-ip>} [<dest-port >]
```

Mode

Global configuration mode

Parameters

group-id: rule group number, range <100-199>|<2000-2699>.
permit: Allow packets that match the rule to be forwarded.
deny: Prohibit packets that match the rule from being forwarded.
remark: adds a comment to the specified rule group.

protocol: The protocol type above the IP layer, e.g. ip, tcp, udp, etc. You can also enter the corresponding number, e.g. 6 for tcp. If you do not need to control these protocols, you can enter ip or (0).
source-ip: source IP, with three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
wildcard: Determines which bits need to be matched, '0' means they need to be matched, '1' means they don't need to be matched.
source-port: is for the case of protocol for tcp or udp, can control the source port of the packet, input can be some familiar port service name, such as: www, can also be a number, such as 80 for www port.
dest-ip: Destination IP address. There are three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
dest-port: For the case of protocol tcp or udp, you can control the destination port of the packet, the input method is the same as srcPort.

Description

Configure an extended ip rule to match specified protocol packets, which can be forwarded or discarded depending on the source and destination IP addresses, message type, or port of the packet.

Examples

Configure the rule to prohibit ip packets from 192.168.0.2 to 192.168.1.0 network segment and allow ospf packets from 192.168.0.2 to 192.168.2.1.

```
Switch(config)#access-list 100 deny ip host 192.168.0.2 192.168.1.0 0.0.0.255
Switch(config)#access-list 100 permit ospf host 192.168.0.2 host 192.168.2.1
```

Configure a set of rules so that addresses in the 10.1.0.0 255.255.0.0 segment cannot access any www servers, but 10.1.1.1 does not have the above restriction; the following configuration can be made.

```
switch# access-list 200 deny tcp 10.1.0.0 0.0.255.255 any www
switch# access-list 200 permit tcp host 10.1.1.1 any www
```

MAC IP-based ACL rules

Command

```
access-list <groupId> {deny | permit | remark} <source-mac> ip <source-ip><destination-ip>
```

Mode

Global configuration mode

Parameters

group-id: rule group number, range 700~799.
permit: Allow packets that match the rule to be forwarded.
deny: Prohibit packets that match the rule from being forwarded.
remark: adds a comment to the specified rule group.
source-mac: source MAC. there are three input methods.
1) HHHH.HHHH.HHHH wildcard can control the MAC address from a network segment.
2) any Equivalent to HHHH.HHHH.HHHH FFFF.FFFF.FFFF
3) host A.B.C.D is equivalent to HHHH.HHHH.HHHH 0000.0000.0000
source-ip: source IP, with three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
wildcard: Determines which bits need to be matched, '0' means they need to be matched, '1' means they don't need to be matched.
dest-ip: Destination IP address. There are three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255

3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

Description
Configure a MAC-based ip rule that can decide to forward or discard packets based on their source and destination IP addresses, source and destination MACs.

Examples
Configure the rule to prohibit IP packets from source MAC address 0009.ca10.0907 with IP 192.168.0.2 to destination MAC address 0009.ca10.0908 with IP 192.168.2.3.

```
Switch(config)#access-list 700 deny host 0009.ca10.0907 host 0009.ca10.0908 ip host 192.168.0.2 host
192.168.0.3
Switch(config)#
```

MAC ARP-based ACL rules

Command

```
access-list <groupId> {deny | permit | remark} arp<sender-mac><sender-ip>
```

Mode
Global configuration mode

Parameters
group-id: rule group number, range 1100~1199.
permit: Allow packets that match the rule to be forwarded.
deny: Prohibit packets that match the rule from being forwarded.
remark: adds a comment to the specified rule group.
sender-mac: The MAC address of the sender.
sender-ip: IP address of the sender.

Description
Configure a MAC ARP-based ACL rule to match specified protocol packets, which can be forwarded or discarded based on the source IP address and source MAC of the packet.

Examples
Configure ACL rule id to 1100, allow mac source address 0009.ca10.1122 and source IP 192.168.0.10 to send arp messages.

```
Switch(config)#access-list 1100 permit arp host 0009.ca10.1122 host 192.168.0.10
Switch(config)#
```

time-range

Command

```
time-range <range-name> cycle-time days from <start-weekdays> to <end-weekdays>
time-range <range-name> cycle-timefrom <start-hour><start-minute> to <end-hour ><end-minute> [days
from < start-weekdays> to <end-weekdays>]
time-range <range-name> utter-time from <start-year><start-month><start-day><start-hour><start-minute
> to <end-year><end-month><end-day><end-hour><end-minute>
no time-range
no time-range<range-name> [cycle-time|utter-time]
```

Mode
Global configuration mode

Parameters
range-name: name of the time period, character length <1-31>.
start-weekdays: the days of the week to start, takes the value <0-6>, 0-Sunday, 1-Monday, 2-Tuesday, 3-Wednesday, 4-Thursday, 5-Friday, 6-Saturday).
end-weekdays: the weekday of the deadline, takes the value <0-6>.
<start-year><start-month><start-day><start-hour><start-minute>: The time and minute of the year, month and day when it starts.
<end-year><end-month><end-day><end-hour><end-minute>: The end date and time of the year and month.

Description
The cycle-time keyword is followed by the time of the cycle.
The utter-time keyword is followed by an absolute time period.

Examples
#No

Time period based ACL rules

Command
```
time-acl<group-id>time-range<range-name>
no acl<group-id>time-range[<range-name>]
```

Mode
Global configuration mode

Parameters
group-id: rule group number.
range-name: name of the time period, character length <1-31>.

Description
The so-and-so acl rule applies for a certain time period and works when the acl is applied to the interface.

Examples
```
#
Switch(config)#time-acl 99 time-range ss
Switch(config)#
```

Issuing ACL rules

Command
```
access-group <group-id>
```

Mode
Interface configuration mode

Parameters
group-id: the referenced rule group number, standard IP rule range <1-99>|<1300-1999>, extended IP rule range <100-199>|<2000-2699>, Mac arp rule range <1100-1199>, Mac ip rule range <700-799>,

Description
Reference a set of acl rules on the port.

Examples
Reference rule group 1 on port ge1/1.
```
Switch(config-ge1/1)#access-group 1
Switch(config-ge1/1)#
```

Delete ACL rules

Command
```
no access-list <group-id>
```

Mode
Global configuration mode

Parameters
group-id: rule group number.

Description
Delete the configured ACL rule.

Examples

Delete ACL rule 1.

```
Switch(config)#no access-list 1
Switch(config)#
```

ACL view command

show access-group

Command

```
show access-group
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

Displays references to acl rules.

Examples

```
#Switch#show access-group
Interface ge1/1
access-list 100 is set
```

show access-list

Command

```
show access-list [<group-id>]
```

Mode

Privilege mode

Parameters

group-id: the rule number to be displayed.

Description

Displays the configured acl rules.

Examples

```
#Switch#show access-list
Standard IP access list 1, Remark acl1
deny 192.168.1.0, wildcard bits 0.0.0.255
permit any
Extended IP access list 100,
permit ospf host 192.168.0.2 host 192.168.2.1
permit ip host 192.168.0.2 192.168.1.0 0.0.0.255
Switch#
```

show time-range

Command

```
show time-range [<range-name> [cycle-time | utter-time]]
```

Mode

Normal mode / Privilege mode

Parameters

range-name: name of the time period, character length <1-31>.

Description

Display such-and-such time period (including all absolute and relative time periods or all time periods).

Examples

Display the time period named time1.

```
Switch#show time-range time1
current time: 2000.01.01 01:05 Saturday
time range time1:
cycle time: 00:00 - 20:00 Sunday - Saturday
Switch#
```

show time-acl

Command

```
show time-acl <group-id | all >time range
```

Mode

Normal mode / Privilege mode

Parameters

group-id: rule group number.

Description

Show all time periods for which such-and-such acl or all rules are applied.

Examples

The time period for which all rules are applied is displayed.

```
Switch>show time-aclall time-range
acl 1100 has related 1 time ranges: 1
Switch>
```

CHAPTER 20

TCP/IP basic commands

Configuration commands

arp

Command

```
arp <ip-address><mac-address>
no arp <ip-address>
```

Mode

Global configuration mode

Parameters

ip-address: the IP address of the binding, expressed in 32-bit dotted decimal.
mac-address: the physical address of the binding, expressed in 12-bit hexadecimal; the mac address, in the format HHHH.HHHH.HHHH.

Description

The arp command is used to configure a static arp table entry. After successful configuration, the data corresponding to the IP and MAC addresses can only be forwarded from the specified Layer 2 port.
The no arp command is used to delete the corresponding arp table entry or static configuration.

Examples

```
#Configure mapping of ip address 192.168.1.1 to MAC address 0003.0010.1011
Switch(config)#arp 192.168.1.1 0003.0010.1011
Switch(config)#
```

ip address

Command

```
ip address <address/mask>
no ip address [<address/mask>]
```

Mode

Interface configuration mode

Parameters

address/mask: ip address and mask length. Value range address:0.0.0.0~223.255.255.255;mask:0~32.

Description

ip address: The command is used to configure an IP address for a Layer 3 interface. This command is currently available only for Layer 3 interfaces (vlan). Use the ip interface vlan command to start the Layer 3 interface before issuing this command.
The no ip address command is used to delete the IP address configured on the interface.

Examples

Configure interface vlan4 with an ip address of 192.168.192.32 and a mask length of 24 bits.

```
Switch#conf ter
Switch(config)#inter vlan24
Switch(config-vlan24)#ip addr 192.168.192.32/24
Switch(config-vlan24)#end
Switch#show ip interface vlan24 brief
Interface IP-Address Status Protocol
vlan24 192.168.192.32 up up
```

```
Switch#
```

ip route

Command

```
ip route {<ip-address>/<mask-length> | <ip-address><mask>} <gateway >
no ip route {<ip-address>/<mask-length> | <ip-address><mask>}
```

Mode

Global configuration mode

Parameters

ip-address: The destination IP address, in 32-bit dotted decimal format.
mask-length: the length of the mask, expressed in decimal.
mask: mask of the IP address, in dotted decimal format.
gateway: IP address of the next-hop gateway for the specified route, in dotted-decimal format.

Description

The ip route command is used to configure a static route and enables route selection and backup of routes according to the control of the distance parameter.
The no ip route command is used to delete static routes. When multiple routes exist to reach the same network, not specifying a gateway will delete all static routes that match the destination network.

Examples

Configure a route to the 210.1.1.0/24 segment with the next hop at 172.20.2.2.

```
Switch#configure terminal
Switch(config)#ip route 210.1.1.0/24 172.20.2.2
Switch(config)#
#delete a static route
Switch#configure terminal
Switch(config)#no ip route 210.1.1.0/24
Switch(config)#
```

ip interface vlan

Command

```
ip interface vlan <vlan-id>
no ip interface vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

vlan-id: vlan id number.

Description

The ip interface vlan command is used to enable a Layer 3 interface.
The no ip interface vlan command is used to cancel the Layer 3 interface.

Examples

```
#Enable the vlan 2 Layer 3 interface to.
Switch(config)#ip interface vlan 2
```

route-map

Command

```
route-map <map-tag> {permit | deny} <sequence>
no route-map <map-tag> {permit | deny} <sequence>
```

Mode

Global configuration mode

Parameters
map-tag: route-map name.
permit: allow to pass.
deny: refuse to pass.
sequence: match the sequence number.

Description
The route-map command is used to create a route-map rule and enter the configuration mode of the rule. The configured route-map rule can be used by rip, ospf, and other protocols to invoke control of routes.
The no route-map command is used to delete one or all of a set of route-map rules.

Examples
```
#Add a pass-through rule for route-map "abc0" with sequence number 10
switch(config)#route-map abc0 permit 10
switch(config-route-map)#
```

Display commands

show arp

Command
```
show arp
```

Mode
Normal mode / Privilege mode

Parameters
None.

Description
Displays the address resolution table.

Examples
Show all arp tables.
```
Switch#show arp
Address HWaddress Interface Type
192.168.0.1 00:09:ca:11:99:23 vlan1 Dynamic
Switch#
```

show ip interface

Command
```
show ip interface [<ifname>] brief
```

Mode
Normal mode / Privilege mode

Parameters
ifname: The interface name interface name to be specified, either a Layer 2 interface or a Layer 3 interface. By default, all Layer 2 and Layer 3 interfaces are displayed.

Description
The show ip interface command is used to display summary information about an interface.

Examples
Display information about interface vlan24.
```
Switch#show ip interface vlan24 brief
Interface IP-Address Status Protocol
vlan24 192.168.192.32 up up
Switch#
```

show ip route

Command

```
show ip route [<network>]
```

Mode

Privilege Mode / Normal Mode

Parameters

Default parameter: Display the routes that are active in the current routing table.
network: Specifies to display the routes of the associated network, expressed in 32-bit dotted decimal or address prefix/mask form.

Description

The show ip rout command is used to display routing information. The content includes destination address, mask length, protocol, priority, weight, next hop, and output interface.
This command displays only the currently active routes (best routes).

Examples

```
#Display the currently used routes
Switch#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
C 192.168.0.0/24 is directly connected, vlan1
Switch#
#Display routes for the specified network
Switch#show ip route 1.0.2.0
Routing entry for 1.0.2.0/24
Known via "static", distance 120, metric 2, best
Last update 00:05:37 ago
* 172.20.1.3, via vlan2
Switch#
```

show ip route database

Command

```
show ip route database
```

Mode

Privilege Mode / Normal Mode

Parameters

Default parameter: Display all routes in the routing table, including active and inactive routes.

Description

The show ip rout database command is used for the entire routing information in the routing table, including inactive routes.

Examples

Show all routes

```
Switch#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
> - selected route, * - FIB route, p - stale info
```

```
S *>0.0.0.0/0 [1/0] via 192.168.0.200, vlan1
C *> 192.168.0.0/24 is directly connected, vlan1
Switch#
```

CHAPTER 21

SNMP commands

SNMP configuration commands

snmp community

Command

```
snmp community <community-name> {ro | rw}
no snmp community <community-name>
```

Mode

Global configuration mode

Parameters

Community-name: SNMP common body name. Character length: 1~20.
ro: read-only attribute.
rw: read/write attribute.

Description

The snmp community command is to configure the SNMP share name and the related attributes of the share.
The no snmp community command is to delete the specified SNMP share body name.

Examples

Configure a shared body named private with a read/write attribute.

```
Switch(config)#snmp community private rw
```

Delete a shared body named private

```
Switch(config)#no snmp community private
```

snmp trap

Command

```
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}
no snmp trap <notify-name>
```

Mode

Global configuration mode

Parameters

notice-name: SNMP trap naming. Character length: 1~32.
Ipaddress: the destination IP address to send the trap to.
1: SNMP version 1.
2: SNMP version 2.
3: SNMP version 3.

Description

The snmp trap command is to configure SNMP trap and the related attributes of this trap.
The no snmp trap command is to delete the specified SNMP trap.

Examples

Configure an SNMP trap named test and the destination IP to be sent is 192.168.0.10; the SNMP version used is 1.

```
Switch(config)#snmp trap test host 192.168.0.10 version 1
```

Delete an SNMP trap named test

```
Switch(config)#no snmp trap test
```

snmp system information

Command

```
snmp system information <contact | location | name >< information string >
no snmp system information <contact | location | name >
```

Mode

Global configuration mode

Parameters

information string: the specified content. Character length: 1~255.

Description

The snmp system information command is to configure system information.
The no snmp system information command is to delete the system information.

Examples

```
#Configure the system's contact with the following specifics: E-mail:networks@AAA.com
Switch(config)#snmp system information contact E-mail:networks@AAA.com
The specific content of the location of the #configuration system is: Shenzhen,
Switch(config)#snmp system information location Shenzhen
#Configure the system name as follows: switch
Switch(config)#snmp system information name switch
#Delete the system name
Switch(config)#no snmp system information name
```

SNMP view command

show snmp community

Command

```
show snmp community
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show snmp community command is to display all the current common body names.

Examples

Show all common body names:

```
Switch# show snmp community
```

show snmp trap

Command

```
show snmp trap
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show snmp trap command is used to display all current trap names.

Examples

Show all trap names:

```
Switch#show snmp trap
```

show snmp system information

Command

```
show snmp system information
```

Mode

Normal mode / Privilege mode

Parameters

None

Description

The show snmp system information command is to display the system information of SNMP settings.

Examples

Displays the current system information:

```
Switch#show snmp system information
```

CHAPTER 22

RMON command

RMON configuration commands

rmon statistics

Command

```
rmon statistics <1-100>[owner<word>]
no rmon statistics <1-100>
```

Mode

Interface configuration mode

Parameters

word: the name of the owner.

Description

The rmon statistics command is used to enable the configuration of a statistics group with the specified serial number, which is an interactive command. The configuration is user can enter the serial number and owner when prompted, where owner is optional. The serial number is the number of the statistics group configuration and takes values from 1 to 100.

Examples

Configure port ge1/2 RMON statistics group.

```
Switch(config-ge1/2)#rmon statistics 1 owner net
Switch(config-ge1/2)#
```

rmon history

Command

```
rmon history <1-100> buckets <1-100> interval <1-3600> [owner<word>]
no rmon history <1-100>
```

Mode

Interface configuration mode

Parameters

word: the name of the owner.

Description

The serial number is the number of the history group configuration and takes values from 1 to 100; the number of request buckets is the maximum number of saved data and takes values from 1 to 100; the sampling interval is in seconds and takes values from 1 to 3600.

Examples

```
#Port ge1/2 RMON history group serial number 3, request bucket size 10, and interval 15 seconds.
Switch(config-ge1/2)#rmon history 3 buckets 10 interval 15
Switch(config-ge1/2)#
```

rmon alarm

Command

```
rmon alarm <alarm-id><ararm-word><1-3600>{ absolute|delta } rising-threshold <1-2147483647><event-id
falling-threshold <1-2147483647><event-id> [owner <word>]
no no rmon alarm < alarm-id>
```

Mode
Global configuration mode

Parameters
alarm-id: Alarm group index number <1-60>.
ararm-word:Monitor object, which is the OID of a MIB node.
event-id: index number of the event group <1-60>.
word: the name of the owner.

Description
The rmon alarm group command contains serial number, monitoring object, time interval, comparison method, upper limit threshold, upper limit event serial number, lower limit threshold, lower limit time serial number and owner. The serial number is the number of the alarm group configuration, and the range is 1 to 60; the monitoring object is the OID of a MIB node, the sampling interval is in seconds, and the range is 1 to 3600; the comparison method can choose absolute or delta, which indicates the absolute value (the value of each sample) and the relative value (the increment of each sample relative to the last sample), respectively; the upper and lower threshold values are The range is from 1 to 2147483647; events must be configured in advance, and the numbering range is from 1 to 60.

Examples
Configure rmon alarm group

```
Switch(config)#rmon event 1 log-trap xiongjm
Switch(config)#rmon alarm 1 3.6.3.1 20 delta rising-threshold 30000 1 falling-threshold 2000 1
Switch(config)#
```

rmon event

Command

```
rmon event <event-id>{log|log-trap<trap-word>|none|trap <trap-word>} [description <string>|owner
<word>]
```

Mode
Global configuration mode

Parameters
event-id: index number of the event group <1-60>.
trap-word:SNMP group name.
string: description character.
word: the name of the owner.

Description
The rmon event group command contains a serial number, event type, common body name, description, and owner. The event type can be log (logging), log-trap (logging and issuing a trap), none (no action), and trap (issuing a trap). When log-trap or trap is selected, the common body name must also be specified (the common body name configuration is ignored in this device) .

Examples
Configure rmon event groups

```
Switch(config)#rmon event 1 log-trap xiongjm
Switch(config)#
```

RMON view command

show rmon

Command

```
show rmon {statistics|history-control|alarm|event} config
```

Mode
Normal mode / Privilege mode

Parameters
None

Description
The show rmon config command is used to view the specific configuration of RMON.

Examples
Show all rmon event groups:

```
Switch#show rmon event config
RMON event configuration
Index :1
```

Description :
Type :log-trap
Community :xiongjm
Owner :
Switch#

show rmon statistics-data interface

Command

```
show rmon statistics-data interface<if-name>
```

Mode
Normal mode / Privilege mode

Parameters
if-name:Specific port.

Description
The show rmon statistics-data interface command is used to view port rmon statistics information.

Examples

```
#
Switch#show rmon statistics-data interface ge1/1
DropEvents :0
Octets :865166
Pkts :6952
BroadcastPkts :81
MulticastPkts :6871
CRCAlignErrors :0
UndersizePkts :0
OversizePkts :0
Fragments :0
Jabbers :0
Collisions :0
Pkts64Octets :4
Pkts65to127Octets :6871
Pkts128to255Octets :21
Pkts256to511Octets :56
Pkts512to1023Octets :0
Pkts1024to1518Octets :0
Switch#
```

show rmon history-data interface

Command

```
show rmon history-data interface<if-name>
```

Mode

Normal mode / Privilege mode

Parameters

if-name:specific port

Description

The show rmon history-data interface command is used to view port rmon statistics.

Examples

```
#
Switch#show rmon history-data interface ge1/2
Index :3
SampleIndex :141
IntervalStart :2011/10/09 01:25:43
DropEvents :0
Octets :0
Pkts :0
BroadcastPkts :0
MulticastPkts :0
CRCAlignErrors :0
UndersizePkts :0
OversizePkts :0
Fragments :0
Jabbers :0
Collisions :0
Utilization :0
Index :3
SampleIndex :140
IntervalStart :2011/10/09 01:25:28
DropEvents :0
Octets :0
Switch#
```

CHAPTER 23

Cluster Configuration

NDP configuration commands

ndp global enable

Command

```
[no] ndp global enable
```

Mode

Global configuration mode.

Parameters

None.

Description

Enabling the global NDP protocol

Examples

```
#start global ndp protocol
Switch#configure terminal
Switch(config)#ndp global enable
Switch(config)#
```

ndp enable

Command

```
[no] ndp enable
```

Mode

Interface configuration mode.

Parameters

None.

Description

Enable port NDP function

Examples

```
#start port ge1/1 ndp protocol
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ndp enable
Switch(config-ge1/1)#
```

ndpaging-timer

Command

```
[no] ndpaging-timer<aging-time>
```

Mode

Global configuration mode.

Parameters

aging-time: Configure the aging time of NDP messages sent by this device on the receiving device. The range is 1-4096, and the default is 180 seconds.

Description
Configure the aging time of NDP messages sent by this device on the receiving device

Examples
```
#Aging time for starting ndp is 100 seconds
Switch#configure terminal
Switch(config)#ndp aging-timer 100
Switch(config)#
```

ndp hello-timer

Command
```
[no] ndp hello-timer<hello-time>
```

Mode
Global configuration mode.

Parameters
hello-time: range 1-4096, default 60 seconds.

Description
Configure the time interval for NDP messages to be sent.

Examples
start ndp hello sending interval is 10 seconds
```
Switch#configure terminal
Switch(config)#ndp hello-timer 10
Switch(config)#
```

show ndp

Command
```
show ndp[ interface <if-name>]
```

Mode
Normal mode / Privilege mode.

Parameters
if-name: The specific interface.

Description
View NDP information.

Examples
```
#View interface ge1/1 ndp information
Switch#show ndp interface ge1/1
Neighbour Discovery Protocol is enabled
Neighbour Discovery Protocol Hello Timer:5(s), Aging Timer:180(s)
Interface:ge1/1
Status:enabled, Pkts Snd:58, Pkts Rvd:37, Pkts Err:0
Neighbour 1: Aging Time:179.933334(s)
MAC address : 0001-ca08-abcf
Host name : SW28
Port name : ge1/1
Port duplex : Full
Version : 5.1.6
Management Vlan: 222
Management :
Telnet; SNMPv2; WEB; TFTP Client;
Switch#
```

reset ndp statistics

Command

```
reset ndp statistics [interface <if-name>]
```

Mode

Global configuration mode.

Parameters

if-name: The specific interface.

Description

Clear NDP statistics.

Examples

Clear NDP statistics for port ge1/1

```
Switch#configure terminal
Switch(config)#reset ndp statistics ge1/1
Switch(config)#
```

NTDP configuration commands

ntdp global enable

Command

```
[no] ntdp global enable
```

Mode

Global configuration mode.

Parameters

None.

Description

Enabling the global NTDP protocol

Examples

```
#start global ntdp protocol
Switch#configure terminal
Switch(config)#ntdp global enable
Switch(config)#
```

ntdp enable

Command

```
[no] ntdp enable
```

Mode

Interface configuration mode.

Parameters

None.

Description

Enable port NTDP function

Examples

```
#start port ge1/1 ntdp protocol
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ntdp enable
Switch(config-ge1/1)#
```

ntdptimer

Command

```
[no] ntdptimer {<time-value>| hop-delay < hop-value> | port-delay < port-value>}
```

Mode

Global configuration mode.

Parameters

time-value: range 0-65535, default 1 minute.
hop-value: range 1-1000, default 200 milliseconds.
port-value: range 1-100, default 20 milliseconds

Description

The ntdptimer command is used to set the time interval for timed topology collection.
The ntdp timer hop-delay command is used to set the time that the collected device waits before forwarding a topology collection request message on the first port.
The ntdp timer port-delay command is used to configure the port delay time for the current device to forward topology collection requests.

Examples

Set the topology collection interval of ntdp to 1 minute

```
Switch#configure terminal
Switch(config)#ntdp timer 1
Switch(config)#
```

ntdp hop

Command

```
[no] ntdp hop <hop-value>
```

Mode

Global configuration mode.

Parameters

hop-value: range 1-6, default 3 hops.

Description

The ntdp hop command is used to configure the range of topology collection. By default, the farthest device in the collected topology is the maximum number of hops away from the topology collection device.

Examples

Set the topology collection of ntdp to a range of 2 hops

```
Switch#configure terminal
Switch(config)#ntdp hop 2
Switch(config)#
```

ntdp explore

Command

```
ntdp explore
```

Mode

Privilege mode.

Parameters

None.

Description

Manually collect topology information once.

Examples

```
#Manual collection of topology information
Switch#ntdp explore
```

show ntdp

Command

```
show ntdp
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

View NTDP configuration information.

Examples

```
#
```

show ntdp device-list

Command

```
show ntdpdevice-list [verbose]
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

View the device information collected by NTDP.

Examples

```
Switch#show ntdp device-list
MAC HOP IP Device
0001-ca08-abcf 0 SW28
Switch#
```

show ntdp single-device mac-address

Command

```
show ntdp single-device mac-address<mac-address>
```

Mode

Normal mode / Privilege mode.

Parameters

mac-address: mac address in the format HHHH.HHHH.

Description

Displays NTDP details for the specified device.

Examples

```
#Display information of the device with MAC address 0009.ca52.d05c
Switch#show ntdp single-device mac-address 0009.ca52.d05c
Hostname : Switch
MAC : 0009-ca52-d05c
Version : 5.1.7
Cluster :
Management Vlan:
```

```
Neighbours:
Peer MAC:0009-ca52-d041
Peer Port ID:ge1/2
Native Port ID:ge1/2
Speed:100m
Duplex:Full(1)
STP state:FORWARDING
Peer MAC:0000-0011-293a
Peer Port ID:ge1/2
Native Port ID:ge1/2
Speed:1g
Duplex:Full(1)
STP state:FORWARDING
Switch#
```

Cluster configuration commands

cluster enable

Command

```
[no] cluster enable
```

Mode

Global configuration mode.

Parameters

None.

Description

Enabling the cluster function

Examples

```
#Start cluster function
Switch#configure terminal
Switch(config)#cluster enable
Switch(config)#
```

cluster management-vlan

Command

```
[no] cluster management-vlan<vlan-id>
```

Mode

Global configuration mode.

Parameters

vlan-id: The specific vlan that needs to be created first.

Description

The default management VLAN is VLAN1.

Examples

Configure management VLAN to 2

```
Switch#configure terminal
Switch(config)#cluster management-vlan 2
Switch(config)#
```

cluster ip-pool

Command

```
[no] cluster ip-pool <ip-net>
```

Mode

Global configuration mode.

Parameters

ip-net: ip network segment, format like 192.168.1.1/24.

Description

Configure the range of private IP addresses used by member devices in the cluster on the device you want to set as the management device.

Examples

Configure the address pool of the cluster to 192.168.0.1/24

```
Switch#configure terminal
Switch(config)#cluster ip-pool 192.168.0.1/24
Switch(config)#
```

cluster build

Command

```
cluster build<name>
cluster delete <name>
```

Mode

Global configuration mode.

Parameters

name: the name of the character.

Description

Manually create and delete clusters, configure the current device as the management device, and also assign a cluster name.

Examples

```
#Create clusters manuallya
Switch#configure terminal
Switch(config)#cluster build a
Switch(config)#
```

cluster auto-build

Command

```
cluster auto-build<name>
```

Mode

Global configuration mode.

Parameters

name: the name of the character.

Description

Automatic cluster creation.
The auto-clustering feature automatically adds all candidate devices found within the specified hop count range to the created cluster.

Examples

```
#Automatic cluster creationb
Switch#configure terminal
```

```
Switch(config)#cluster build b
Switch(config)#
```

clusterstop auto-add member

Command

```
cluster stop auto-add member
```

Mode

Global configuration mode.

Parameters

None.

Description

Stops the automatic joining of member switches under the auto-create cluster configuration. This operation can only stop joining new devices, devices that have already joined the cluster will remain in the cluster.

Examples

```
#No
```

cluster timer

Command

```
[no] cluster timer <interval-time>
```

Mode

Global configuration mode.

Parameters

interval-time: the value range is 1-255, the default is 10 seconds.

Description

Configure the time interval for handshake messages to be sent.

Examples

Configure the handshake message sending interval to 10 seconds

```
Switch#configure terminal
Switch(config)#cluster time 10
Switch(config)#
```

cluster holdtime

Command

```
[no] cluster holdtime<hold-time>
```

Mode

Global configuration mode.

Parameters

hold-time: value range 1-255, default 60 seconds.

Description

Configure the effective retention time of the device.

Examples

Configure the device with an effective retention time of 60 seconds

```
Switch#configure terminal
Switch(config)#cluster holdtime 60
Switch(config)#
```

cluster add member mac-address

Command

```
cluster add member mac-address <mac-address>
cluster delete member mac-address <mac-address>
```

Mode

Global configuration mode.

Parameters

mac-address: mac address, format HHHH.HHHH.

Description

Add candidate devices to the cluster or remove them.

Examples

```
#Manually add a member device with a MAC address of 0009.ca52.d05c
Switch#configure terminal
Switch(config)#cluster add member mac-address 0009.ca52.d05c
Switch(config)#
```

cluster Switch-to member

Command

```
cluster Switch-to member<member-num>
```

Mode

Privilege mode.

Parameters

member-num: The specific device number.

Description

Switch from the management device operation interface to the member device operation interface.

Examples

```
#Switch from management device to member device 1
Switch#cluster Switch-to member 1
ready connecting to 10.0.0.6 .....
User Access Verification
Switch>
```

Cluster display commands

show cluster

Command

```
show cluster
```

Mode

Normal mode / Privilege mode.

Parameters

None.

Description

Displays the status and statistics of the cluster to which the device belongs.

Examples

```
#
Switch#show clucluster
Cluster name:eeeeee
```

```
Role:Administrator
Management-vlan:222
Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:211.1.1.23/24
Cluster-mac:0180-c200-000a
3 member(s) in the cluster, and 0 of them down.
Switch#
```

show cluster topology

Command

```
show cluster topology
```

Mode

Privilege mode.

Parameters

None.

Description

Displays cluster topology information.

Examples

```
Switch#show cluster topology
-------------------------------------------------------------------
(PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-------------------------------------------------------------------
ConnectFlag:
<--> normal connect ---> odd connect
++++ candidater device -||- STP discarding
-------------------------------------------------------------------
[xiongjmjm_0.SysName:09-ca52-d027]
|
|--(ge1/2)<-->(ge1/2)[xiongjmjm_1.SysName:01-ca8-abcf]
| |
|--(ge1/2)<-->(ge1/2)[xiongjmjm_0.SysName:09-ca52-d027]
Switch#
```

show cluster candidates

Command

```
show cluster candidates [ mac-address <mac-address> ]
```

Mode

Privilege mode.

Parameters

mac-address: mac address, format HHHH.HHHH.

Description

Displays candidate device information.

Examples

```
#Display all candidate device information
Switch#show cluster candidates
MAC HOP IP Device
Switch#
```

show cluster member

Command

```
show cluster member [<mem-number> ]
```

Mode

Privilege mode.

Parameters

mem-number: specific member device index number.

Description

Displays cluster membership information.

Examples

```
#Display all member device information
Switch#show cluster member
SN Device Status IP Name
1 0009-ca52-d05c Up 10.0.0.6/24 Switch
2 0009-ca52-d041 Up 10.0.0.8/24 Switch
Switch#
```

Cluster debugging commands

debug cluster

Command

```
debug cluster [all | conn-fsm |fsm |timer | normal]
```

Mode

Privilege mode.

Parameters

None.

Description

debug cluster is used to turn on the debug switch related to the cluster protocol and write the related logs to the log table.

Examples

```
Switch#debug cluster all
Switch#
```

debug cluster packet

Command

```
debug cluster packet [cm | ndp |ntdp]
```

Mode

Privilege mode.

Parameters

None.

Description

debug cluster packet is used to turn on the debug switch related to cluster packets and write the related logs to the log table.

Examples

```
Switch#debug cluster packet
Switch#
```

CHAPTER 24

SNTP commands

SNTP configuration commands

sntp disable

Command

```
sntp disable
```

Mode

Global configuration mode

Parameters

None.

Description

Turn off the sntp protocol.

Examples

```
#close sntp protocol
Switch#configure terminal
Switch(config)#sntp disable
Switch(config)#
```

sntp enable

Command

```
sntp enable
```

Mode

Global configuration mode

Parameters

None.

Description

Start the sntp protocol.

Examples

```
#start sntp protocol
Switch#configure terminal
Switch(config)#sntp enable
Switch(config)#
```

sntp server

Command

```
sntp server <ip-address>
no sntp server [ip-address]
```

Mode

Global configuration mode

Parameters

ip-address: IP address of the sntp server, expressed in 32-bit dotted decimal.

Description
The sntp server command is to configure the IP address of the sntp server, up to 3 addresses can be set.
The no sntp server command is to delete the IP address of the sntp server.

Examples
```
#Configure the sntp server address to 192.43.244.18
Switch#configure terminal
Switch(config)#sntp server 192.43.244.18
```

sntp interval

Command
```
sntp interval< interval >
no sntp interval
```

Mode
Global configuration mode

Parameters
interval: the interval of the timed synchronization clock, the default is 1800 seconds.

Description
The sntp interval command is to set the interval of timing synchronization clock in seconds, the range is 60-65535.
The no sntp interval command is to restore the interval of the timed synchronization clock.

Examples
Configure the sntp timer to synchronize the clock at an interval of 60 seconds
```
Switch#configure terminal
Switch(config)#sntp interval 60
```

sntp time-zone

Command
```
sntp time-zone< time-zone >
no sntp time-zone
```

Mode
Global configuration mode

Parameters
time-zone: set the time zone, range: -12-12 default is +8 that is, the eastern eight.

Description
The sntp time-zone command is to set the local time zone.
The no sntp time-zone command is to restore the local time zone to East 8.

Examples
Configure local time zone as West 8
```
Switch#configure terminal
Switch(config)# sntp time-zone -8
```

SNTP view command

show sntp

Command
```
show sntp
```

Mode
Normal mode / Privilege mode

Parameters

None.

Description

The show sntp command is to display the configuration information and the current fetch time.

Examples

```
#Display information of sntp
Switch#show sntp
SNTP Server IP: 192.43.244.18
SNTP Interval: 1800s
SNTP Time Zone: GMT+8
SNTP Status: Enabled
SNTP Last Update time: 2011/06/15 15:09:56
System Date Time: 2011/06/15 15:09:59
```

CHAPTER 25

IGMP commands

IGMP configuration commands

ip igmp

Command

```
ip igmp
no ip igmp
```

Mode

Interface configuration mode

Parameters

None.

Description

The ip igmp command is to start the igmp function for this vlan.
The no ip igmp command is to disable the igmp function for this vlan.

Examples

Turn on IGMP function in VLAN1

```
switch(config-vlan1)#ip igmp
```

Disable IGMP function in VLAN1.

```
switch(config-vlan1)#no ip igmp
```

ip igmp access-group

Command

```
ip igmp access-group {<acl-num> | <acl-name>}
no ip igmp access-group
```

Mode

Interface configuration mode

Parameters

acl-num: Access control list number, must be a standard access control list of <1-99>.
acl-name; the name of the access control list.

Description

The ip igmp access-group command turns on IGMP interface group filtering according to the access-list rule.
The no ip igmp access-group command disables the IGMP interface group filtering function.

Examples

```
#Start IGMP filtering for vlan1, filter entries according to access-list 1.
switch(config-vlan1)#ip igmp access-group 1
```

Disable IGMP group filtering for vlan1.

```
switch(config-vlan1)#no ip igmp access-group
```

ip igmp immediate-leave group-list

Command

```
ip igmp immediate-leave group-list {<acl-num1>| <acl-num2>| <acl-name>}
no ip igmp immediate-leave
```

Mode
Interface configuration mode

Parameters
acl-num1: Access control column number, which is a standard access control list numbered <1-99>.
acl-num2: Access control column extension number, a list of standard access control extensions numbered <1300-1999>.
acl-name; the name of the access control list.

Description
The ip igmp immediate-leave group-list command is configured to filter the interface from receiving version 2 and version 3
The multicast address to filter when leaving a message
The no ip igmp immediate-leave command disables the ability to filter the multicast address of the leave message

Examples
Configure the interface of VLAN1 to filter the multicast address of leaving messages that match rule 1

```
switch(config-vlan1)#ip igmp immediate-leave group-list 1
#Disable filtering of leave message multicast addresses for VLAN1
switch(config-vlan1)#no ip igmp immediate-leave
```

igmp last-member-query-count

Command

```
ip igmp last-member-query-count <L-M-Q-Count-value>
no ip igmp last-member-query-count
```

Mode
Interface configuration mode

Parameters
L-M-Q-Count-value: the number of queries for a specific group. Default value: 2, the range of values is: 2~7.

Description
The ip igmp last-member-query-count command is to configure the value of the number of times a particular group is queried
The no ip igmp last-member-query-count command restores the value of this count to its default value.

Examples
Set the IGMP group-specific query count value within VLAN1 to 7.

```
switch(config-vlan1)#ip igmp last-member-query-count 7
#Restore the IGMP group-specific query count value within VLAN1 to its default value
switch(config-vlan1)#no ip igmp last-member-query-count
```

ip igmp last-member-query-interval

Command

```
ip igmp last-member-query-interval <L-M-Q-Interval-value >
no ip igmp last-member-query-interval
```

Mode
Interface configuration mode

Parameters
L-M-Query-Interval-value: group-specific query interval time. Default value: 1000ms, take value
The range is: 1000~25500ms.

Description
The ip igmp last-member-query-interval command is to configure the interval when a group-specific query message is sent

The no ip igmp last-member-query-interval command restores this interval to its default value

Examples

Configure the interval for sending group-specific query messages to 2000ms

```
switch(config-vlan1)#ip igmp last-member-query-interval 2000
#Restore this interval to its default value
switch(config-vlan1)#no ip igmp last-member-query-interval
```

ip igmp querier-timeout

Command

```
ip igmp querier-timeout <timeout-value >
no ip igmp querier-timeout
```

Mode

Interface configuration mode

Parameters

timeout-value :Non-querier timer time. Default value: 255s, the value range is: 60~300s.

Description

The ip igmp querier-timeout command is to configure the non-querier timer time.
The no ip igmp querier-timeout command is to restore the default value.

Examples

Configure the non-querier timer time for vlan1 to 60s.

```
switch(config-vlan1)#ip igmp querier-timeout 60
#Restore the non-querier timer time for vlan1 to the default value of.
switch(config-vlan1)#no ip igmp querier-timeout
```

ip igmp query-interval

Command

```
ip igmp query-interval <Interval-value>
no ip igmp query-interval
```

Mode

Interface configuration mode

Parameters

Interval-value: the interval time for sending query messages. Default value: 125s, the value range is: 1~18000s.

Description

The ip igmp query-interval command is to configure the interval for sending query messages.
The no ip igmp query-interval command restores the interval to its default value

Examples

Set the interval for VLAN1 to send query messages to 100s.

```
switch(config-vlan1)#ip igmp query-interval 100
```

Recovery interval is the default value

```
switch(config-vlan1)#no ip igmp query-interval
```

ip igmp query-max-response-time

Command

```
ip igmp query-max-response-time <response-time>
no ip igmp query-max-response-time
```

Mode

Interface configuration mode

Parameters

respone-time: The maximum response time in IGMP query messages. Default value: 10s, the range of values is 1~240s.

Description

The ip igmp query-max-response-time command is to configure the maximum response time in an IGMP query message.

The no ip igmp query-max-response-time command restores the maximum response time to its default value

Examples

Set the maximum response time in IGMP query messages for VLAN1 to 20s.

```
switch(config-vlan1)#ip igmp query-max-response-time 20
The maximum response time in the #RecoveryQuery message is the default value
switch(config-vlan1)#no ip igmp query-max-response-time
```

ip igmp robustness-variable

Command

```
ip igmp robustness-variable <Robust-value>
no ip igmp robust-variable
```

Mode

Interface configuration mode

Parameters

Robust-value: IGMP robustness factor, the number of retransmissions of IGMP-specific group query messages sent when IGMP receives a leave message. Default value: 2, the range of values is 2~7.

Description

The ip igmp robustness-variable command is to configure the number of times an IGMP-specific group query message is sent when IGMP receives a leave message.

The no ip igmp robustness-variable command restores the send count to its default value

Examples

Set the number of IGMP send specific group queries for VLAN1 to 4.

```
switch(config-vlan1)#ip igmp robustness-variable 4
```

Restore the IGMP send specific group query count for VLAN1 to its default value

```
switch(config-vlan1)#no ip igmp robustness-variable
```

ip igmp version

Command

```
ip igmp version <Version Number>
no ip igmp version
```

Mode

Interface configuration mode

Parameters

Version Number: IGMP version number. Default value: 3, the value range is 1~3.

Description

The ip igmp version command is to configure the version of running IGMP.

The no ip igmp version command restores the send query message version to its default value

Examples

Set the version of the IGMP send query message for VLAN1 to 2.

```
switch(config-vlan1)#ip igmp version 2
```

Restore the version of IGMP send query messages for VLAN1 to the default value

```
switch(config-vlan1)#no ip igmp version
```

IGMP view command

show ip igmp groups

Command

```
show ip igmp groups [<A.B.C.D> [detail] | <interface-name> [<A.B.C.D> [detail] | detail ]
```

Mode

Normal mode / Privilege mode

Parameters

A.B.C.D: Multicast group address
interface: Specifies the interface. This refers to the VLAN interface.

Description

The show igmp group command is to display the relevant multicast group information.

Examples

Display information about the igmp group that exists.

```
switch#show ip igmp groups
```

show ip igmp interface

Command

```
show ip igmp interface [<if-name>]
```

Mode

Normal mode / Privilege mode

Parameters

if-name: Specifies the interface. The VLAN interface is specified here.

Description

The show ip igmp interface command is to display IGMP interface configuration information.

Examples

Display IGMP configuration information for vlan3.

```
switch#show ip igmp interface vlan3
switch#
```

IGMP debug commands

debug igmp

Command

```
debug igmp [all] | [events] | [fsm] | [packet] | [tib]
no debug igmp [all] | [events] | [fsm] | [packet] | [tib]
```

Mode

Privilege mode.

Parameters

all: Turn on all debug switches of igmp.
events: Turn on igmp event debug switch.
fsm: IGMP interface limited state machine
packet: Turn on the igmp message debug switch.
tib: IGMP information status table

Description

The debug igmp command is used to turn on the igmp-related debug switch, enabling the user to see the igmp-related events and messages sent and received.
The no debug igmp command disables the corresponding igmp debug switch.

Examples

Turn on the igmp message debug switch.

```
switch#debug igmp packet
switch#
```

show debug igmp

Command

```
show debug igmp
```

Mode

Normal mode / Privilege mode

Parameters

None.

Description

The show debug igmp command is used to display the status of igmp-related debug switches.

Examples

Display igmp message debug switch status.

```
switch#show debug igmp
switch#
```

CHAPTER 26

PIM-SM Command

System configuration commands

ip mroute

Command

```
Ip mroute <source-address><group-address><iif-name><oif-name>{add | remove}<L2-port>
```

Mode

Global configuration mode

Parameters

source-address: the corresponding source IP address in the multicast route (S,G).
group-address: multicast group address, used to specify a multicast group, the value range is 224.0.0.0~239.255.255.255;
iif-name: the name of the incoming interface for multicast routing, which must be a Layer 3 vlan interface.
oif-name: the name of the outgoing interface for multicast routing, which must be a Layer 3 vlan interface.
L2-port: The Layer 2 port that needs to be added to or removed from the forwarding port list. It can be a Trunk port group, but cannot be a member port of a Trunk group.

Description

On iSpirit 8800 Series switches, the presence of an active multicast route sets all Layer 2 ports within a Layer 3 interface to the forwarding state. ip mroute command is used to manually configure which Layer 2 ports within a Layer 3 interface are active for multicast. source-address, group-address, and iif-name uniquely identifies a multicast route. When oif-name contains multiple Layer 2 ports, the ip mroute command is used to add or remove the specified Layer 2 port from the forwarding list.

Examples

There is interface vlan3, containing Layer 2 ports ge1/0/4, ge4/0/5 and ge4/0/6. For data flows coming in from group vlan2 (192.168.1.12,224.1.1.10), only forwarding from ge1/0/4 is allowed when vlan3 is the outgoing interface.

```
switch(config)#ip mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 remove ge4/0/5
switch(config)#i p mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 remove ge4/0/6
switch(config)#
```

The user of ge1/0/5 is allowed to receive this data stream by requesting, under the above conditions.

```
switch(config)#ip mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 add ge1/0/5
switch(config)#
```

ip multicast route-limit

Command

```
ip multicast route-limit <max-num> [<alarm-num>]
no ip multicast route-limit
```

Mode

Configuration mode.

Parameters

max-num: the upper limit value of multicast routing; the value range is 1 to 2147483647.
alarm-num: The number of multicast routes for which an alarm is issued, in the range of 1 to 2147483647.

Description

The ip ip multicast route-limit command is used to configure the multicast route limit and the number of alarms to be issued; no more multicast routes will be added after the limit is exceeded, and an alarm message will be issued when the alarm value is reached.
The no ip ip multicast route-limit command is used to remove the limit on the number of multicast routes.

Examples

Configure the system to allow up to 300 multicast routes, with alarms issued when 250 are reached.

```
switch(config)#ip multicast route-limit 300 250
switch(config)#
```

ip multicast-routing

Command

```
ip multicast-routing
no ip multicast-routing
```

Mode

Configuration mode.

Parameters

None

Description

the ip multicast-routing command is used to start the multicast routing function of the system.
The no ip multicast-routing command is used to disable the multicast routing function.

Examples

Start the system's multicast routing function.

```
switch(config)#ip multicast-routing
switch(config)#
```

ip pim accept-register

Command

```
ip pim accept-register {list} {<acl-num> | <acl-name>}
no ip pim accept-register
```

Mode

Configuration mode.

Parameters

acl-num: Access control list number, must be an extended access control list of <100-199> or <2000-2699>.
acl-name; the name of the access control list.

Description

The ip pim accept-register command is used to configure a registration filter so that only registration messages containing source addresses that pass ACL filtering will be processed.
The no ip pim accept-register command is used to cancel the registrant filtering configuration.

Examples

Invoke the access control list named reg-filter to filter registrants by.

```
switch(config)#ip pim accept-register list reg-filter
switch(config)#access-list reg-filter permit 192.168.10.1/32
switch(config)#access-list reg-filter deny any
switch(config)#end
switch#show access-list
String IP access list reg-filter,
permit 192.168.10.1/32
deny any
switch#
```

ip pim bsr-candidate

Command

```
ip pim bsr-candidate {<if-name>} [<mask-len>]
no ip pim bsr-candidate
```

Mode

Configuration mode.

Parameters

if-name: specifies the name of the interface that needs to participate in the BSR election.
mask-len: the length of the mask used for bsr calculation, in the range 0 to 32.

Description

The ip pim bsr-candidate command is used to configure an interface to use its ip address as the C-BSR to participate in the BSR election.
The no ip pim bsr-candidate command is used to cancel the C-BSR designation of an interface

Examples

Configure the address of local interface vlan4 to participate in the election of BSR

```
switch(config)#ip pim bsr-candidate vlan4
switch(config)#
```

ip pim cisco-register-checksum

Command

```
ip pim cisco-register-checksum [group-list <acl-num> | <acl-name>]
no ip pim cisco-register-checksum [group-list <acl-num> | <acl-name>]
```

Mode

Configuration mode.

Parameters

acl-num: Access control list number, must be a standard access control list of <1-99> or <1300-1999>.
acl-name; the name of the access control list.

Description

The ip pim cisco-register-checksum command is used to configure the system to be compatible with Cisco's message checksum feature for groups that have passed ACL filtering. This command is valid for all groups when ACL rules are not used.
The no ip pim cisco-register-checksum command is used to remove the configuration of the system-compatible Cisco message checksum inspection feature.

Examples

Configure the registration checksum mechanism for all groups compatible with Cisco.

```
switch(config)#ip pim cisco-register-checksum
switch(config)#
```

ip pim crp-cisco-prefix

Command

```
ip pim crp-cisco-prefix
no ip pim crp-cisco-prefix
```

Mode

Configuration mode.

Parameters

`None.

Description
The ip pim crp-cisco-prefix command is used to configure the interface on which C-RP is initiated to be compatible with Cisco's BSR.
The no ip pim crp-cisco-prefix command is used to remove a compatible Cisco device as a BSR.

Examples
Configure the system to be compatible with Cisco devices as BSRs.
```
switch(config)#ip pim crp-cisco-prefix
switch(config)#
```

ip pim ignore-rp-set-priority

Command
```
ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority
```

Mode
Configuration mode.

Parameters
None.

Description
The ip pim ignore-rp-set-priority command is used to configure the system to ignore the priority of an RP when receiving an RP-Set.
no ip pim ignore-rp-set-priority is used to remove the configuration that ignores RP-Set priority and revert to the default configuration that checks the priority of the RP.

Examples
Configure the system to ignore the priority of the RP-Set.
```
switch(config)#ip pim ignore-rp-set-priority
switch(config)#
```

ip pim jp-timer

Command
```
ip pim jp-timer <jp-interval>
no ip pim jp-timer [<jp-interval>]
```

Mode
Configuration mode.

Parameters
jp-interval: the time interval for sending join/prune messages; the range of values is 1 to 65535; the default value is 60 seconds.

Description
The ip pim jp-timer command is used to configure the time interval of the system periodic join/prune message timer.
The no ip pim jp-timer command is used to restore the system periodic join/prune message timer interval to the default value.

Examples
Configure the system to send join/prune messages at an interval of 75 seconds.
```
switch(config)#ip pim jp-timer 75
switch(config)#
```

ip pim register-rate-limit

Command

```
ip pim register-rate-limit <rate-value>
no ip pim register-rate-limit
```

Mode

Configuration mode.

Parameters

rate-value: the upper rate limit of the received registration message, the message is discarded when the value is exceeded; the value ranges from 1 to 65535; the default does not limit.

Description

The ip pim register-rate-limit command is used to configure the maximum rate at which the system can receive registration messages, and a smaller value can reduce the CPU load to some extent.
The no ip pim register-rate-limit command is used to revert to the default situation, where no limit is placed on the registration message rate.

Examples

Configure the maximum rate of receiving registration messages to 1000pkt/s

```
switch(config)#ip pim register-rate-limit 1000
switch(config)#
```

ip pim register-rp-reachability

Command

```
ip pim register-rp-reachability
no ip pim register-rp-reachability
```

Mode

Configuration mode.

Parameters

None.

Description

The ip pim register-rp-reachability command is used to configure the system to initiate RP reachability checks.
The no ip pim register-rp-reachability command is used to revert to the default situation where RP reachability is not checked.

Examples

Configure the system to start the RP reachability check function.

```
switch(config)#ip pim register-rp-reachability
switch(config)#
```

ip pim register-source

Command

```
ip pim register-source {<ip-address> | <if-name>}
no ip pim register-source
```

Mode

Configuration mode.

Parameters

ip-address: 32-bit dotted decimal ip address.
if-name: The name of the interface.

Description

The ip pim register-source command is used to specify an ip address (or the ip address of a specified interface) as the original address to be encapsulated when sending a registration message; by default, the real interface address to which the registration message is sent is used.
The no ip pim register-source command is used to restore to the default configuration.

Examples
Configure the address of the encapsulated interface vlan1024 as the source address when sending registration messages.

```
switch(config)#ip pim register-source vlan1024
switch(config)#
```

ip pim register-suppression

Command

```
ip pim register-suppression <timer-value>
no ip pim register-suppression
```

Mode
Configuration mode.

Parameters
timer-value: the time value of the timer in seconds, the range: 1-65535; the default value is 60 seconds.

Description
The ip pim register-suppression command is used to configure the suppression time of the registration suppression timer.
The no ip pim register-suppression command is used to restore the value of the registration suppression timer to the default configuration.

Examples
Configure the registration inhibit timer with an inhibit time of 300 seconds.

```
switch(config)#ip pim register-suppression 300
switch(config)#
```

ip pim rp-address

Command

```
ip pim rp-address <ip-address> [<acl-num> | <acl-name>]
no ip pim rp-address <ip-address> [<acl-num> | <acl-name>]
```

Mode
Configuration mode.

Parameters
acl-num: Access control list number, must be a standard access control list of <1-99> or <1300-1999>.
acl-name; the name of the access control list.

Description
The ip pim rp-address command statically configures RP for groups filtered by access control lists, and this RP configuration is valid for all groups when access control lists are not used.
The no ip pim rp-address command removes the corresponding static RP configuration.

Examples
Configure all groups to use static RP 192.168.93.3.

```
switch(config)#ip pim rp-address 192.168.93.3
switch(config)#
```

ip pim rp-candidate

Command

```
ip pim rp-candidate <if-name> [group-list <acl-num> | <acl-name>] [interval <adv-interval>] [priority
<priority- value>]
no ip pim rp-candidate <if-name>
```

Mode

Configuration mode.

Parameters

if-name: Interface name.
acl-num: Access control list number, must be a standard access control list from 1-99.
acl-name; the name of the access control list.
adv-interval: the notification period of C-RP-Adv message, in seconds, the value range is 1 to 16383.
priority-value: priority, the value range is 0 to 255.

Description

The ip pim rp-candidate command is used to configure an interface as a C-RP (candidate RP) while specifying the parameters of the C-RP.
The no ip pim rp-candidate command removes the configuration of the candidate RP.

Examples

Configure vlan4 to use the default parameters as candidate RPs.

```
switch(config)#ip pim rp-candidate vlan4
switch(config)#
```

ip pim rp-register-kat

Command

```
ip pim rp-register-kat <kat-value>
no ip pim rp-register-kat
```

Mode

Configuration mode.

Parameters

kat-value: the value of keep-alive time, the value range is 1 to 65535.

Description

The ip pim rp-register-kat command is used to configure the registration keep-alive time.
The no ip pim rp-register-kat command is used to restore the registration retention time to the default value.

Examples

Configure registrant retention time to 250 seconds.

```
switch(config)#ip pim rp-register-kat 250
switch(config)#
```

ip pim spt-threshold

Command

```
ip pim spt-threshold [group-list <acl-num | acl-name>]
no ip pim spt-threshold [group-list <acl-num | acl-name>]
```

Mode

Configuration mode.

Parameters

Default: switching of multicast routes for all groups.
acl-num: Access control list number, must be a standard access control list of <1-99> or <1300-1999>.
acl-name; the name of the access control list.

Description

The ip pim spt-threshold command is used to configure the threshold value for PIM-SM switching from RPT to SPT. the default is unconditional switching, that is, the threshold value is 0. By default, all groups switch to SPT unconditionally.

The no ip pim spt-threshold command is used to remove the switching configuration.

Examples

Configure to control only group 234.1.1.1 to SPT switching via grp-list.

```
switch(config)#ip pim spt-threshold group-list grp-list
switch(config)#access-list grp-list per 234.1.1.1/32
switch(config)#
```

Interface configuration commands

ip pim dr-priority

Command

```
ip pim dr-priority <priority>
no ip pim dr-priority [<priority>]
```

Mode

Interface configuration mode.

Parameters

priority: The priority value used by the interface for DR election. Value range: 0 to 4294967294, the default value is 1.

Description

The ip pim dr-priority command is used to configure the priority value to be used when this interface participates in DR elections.

The no ip pim dr-priority command is used to restore the default value of 1 to be used when the interface participates in DR elections.

Examples

Configure the DR priority of interface vlan10 to 123

```
switch(config)#interface vlan100
switch(config-vlan100)#ip pim dr-priority 123
switch(config-vlan100)#end
switch#show ip pim sparse-mode interface detail
vlan100 (vif 3):
Address 192.168.100.1, DR 192.168.100.1
Hello period 30 seconds, Next Hello in 13 seconds
Triggered Hello period 5 seconds
Neighbors:
switch#
```

ip pim exclude-genid

Command

```
ip pim exclude-genid
no ip pim exclude-genid
```

Mode

Interface configuration mode.

Parameters

None.

Description
The ip pim exclude-genid command is used to configure the locally sent PIM-SM hello message to exclude the Gen-id, which is included by default.
The no ip pim exclude-genid command is used to revert to the default configuration without including the gen-id in the hello.

Examples
```
#Enable vlan10 on
switch(config-vlan10)#ip pim exclude-genid
switch(config-vlan10)#
```

ip pim hello-holdtime

Command
```
ip pim hello-holdtime <holdtime>
no ip pim hello-holdtime
```

Mode
Interface configuration mode.

Parameters
holdtime: The valid timer time for hello messages on the interface. The unit is seconds. Value range: 1 to 65535; default value is 105 seconds.

Description
The ip pim hello-holdtime command is used to configure the hold time for hello messages, starting from the last hello message received from a neighbor, and assuming that the neighbor no longer exists if no hello message is received after the timeout.
The no ip pim hello-holdtime command is used to restore the hello message hold time to its default value.

Examples
Configure hello-holdtime for interface vlan100 to 123 seconds
```
switch(config)#interface vlan100
switch(config-vlan100)#ip pim hello-holdtime 123
switch(config-vlan100)#
```

ip pim hello-interval

Command
```
ip pim hello-interval <interval>
no ip pim hello-interval
```

Mode
Interface configuration mode.

Parameters
interval: the time interval for sending hello messages periodically, in seconds. Value range: 1-65535; default: 30 seconds.

Description
The ip pim hello-interval command is used to configure the time interval for hello messages to be sent on an interface.
The no ip pim hello-interval command is used to remove the time configuration for hello messages to be sent on the interface and restore it to the default value.

Examples
Configure the hello-interval time for interface vlan100 to 25 seconds
```
switch(config)#inter vlan100
switch(config-vlan100)#ip pim hello-intervla 25
switch(config-vlan100)#end
```

```
switch# show ip pim sparse-mode interface detail
vlan100 (vif 3):
Address 192.168.100.1, DR 192.168.100.1
Hello period 25 seconds, Next Hello in 18 seconds
Triggered Hello period 5 seconds
Neighbors:
switch#
```

ip pim neighbor-filter

Command

```
ip pim neighbor-filter {< acl-num> | <acl-name>}
no ip pim neighbor-filter {< acl-num> | <acl-name>}
```

Mode

Interface configuration mode.

Parameters

acl-num: Access control list number, must be a standard access control list of <1-99>.
acl-name; the name of the access control list.

Description

The ip pim neighbor-filter command is used to configure neighbor filtering on an interface so that routers that have passed the access control list filter can become local neighbors.
The no ip pim neighbor-filter command is used to restore the delete neighbor filtering configuration without filtering on neighbors.

Examples

Configure the access control list named simple on interface vlan100 to filter on neighbors and deny ip addresses 192.168.100.4 to 192.168.100.7 as their own neighbors.

```
switch(config)#access-list simple deny 192.168.100.4/30
switch(config)#access-list simple permit any
switch(config)#interface vlan100
switch(config-vlan100)#ip pim neighbor-filter simple
switch(config-vlan100)#
```

ip pim sparse-mode

Command

```
ip pim sparse-mode
no ip pim sparse-mode
```

Mode

Interface configuration mode.

Parameters

None.

Description

The ip pim sparse-mode command is used to enable the PIM-SM function of an interface.
The no ip pim sparse-mode command is used to disable the PIM-SM function of an interface.

Examples

```
#Enable PIM-SM on interface vlan100.
switch(config-vlan100)#ip pim sparse-mode
switch(config-vlan100)#
```

ip pim sparse-mode passive

Command

```
ip pim sparse-mode passive
no ip pim sparse-mode passive
```

Mode

Interface configuration mode.

Parameters

None.

Description

The ip pim sparse-mode passive command is used to enable the PIM-SM suppression function on an interface. After configuration, the interface can normally process incoming PIM-SM protocol messages, but does not send PIM-SM protocol messages.

The no ip pim sparse-mode passive command is used to disable the PIM-SM suppression function of the interface.

Examples

```
#Enable PIM-SM interface suppression on interface vlan100.
switch(config-vlan100)#ip pim sparse-mode passive
switch(config-vlan100)#
```

ip multicast ttl-threshold

Command

```
ip multicast ttl-threshold <ttl-value>
no ip multicast ttl-threshold
```

Mode

Interface configuration mode.

Parameters

ttl-value: Specifies the ttl value of the multicast routing output interface list, in the range of 0 to 255; the default value is 255.

Description

The ip multicast ttl-threshold command is used to configure the TTL value of ip packets when encapsulating multicast packets on an interface, and limit the range of packet delivery by the TTL value.

The no ip multicast ttl-threshold command is used to restore the TTL value of multicast message encapsulation on an interface to the default value.

Examples

Configure multicast ip packet TTL value of 10 on interface vlan100.

```
switch(config-vlan100)# ip multicast ttl-threshold 10
switch(config-vlan100)#
View command
```

show debugging pim sparse-mode

Command

```
show debugging pim sparse-mode
```

Mode

Normal mode/privileged mode.

Parameters

None.

Description

The show debugging pim sparse-mode command is used to display the open status of each debugging switch of PIM-SM.

Examples

Displays the PIM-SM debug switch currently turned on by the system.

```
switch#show debugging pim sparse-mode
PIM-SM debugging status:
PIM event debugging is on
PIM packet debugging is on
switch#
```

show ip mroute

Command

```
show ip mroute [<ip-address> | count | dense | sparse | summary]
```

Mode

Normal mode/privileged mode.

Parameters

Default: Display all multicast routing information
ip-address: group address or source address, 32 decimal points.
count: the number of multicast routes counted.
dense: PIM-intensive mode (PIM-DM).
sparse: PIM sparse mode (PIM-SM).
summary: Simple summary information.

Description

The show ip mroute command is used to display multicast routing information including the source, group address, inbound interface list, outbound interface list, and related timer information for multicast routes.

Examples

Display the current sparse mode multicast routing information.

```
switch#show ip mrout sparse
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
StateInterface: Interface (TTL)
(192.168.77.3, 233.1.1.1), uptime 00:01:04, stat expires 00:03:24
Owner PIM-SM, Flags: TF
Incoming interface: vlan400
Outgoing interface list:
vlan1024 (1)
(192.168.77.3, 233.1.1.2), uptime 00:01:04, stat expires 00:03:24
Owner PIM-SM, Flags: TF
Incoming interface: vlan400
Outgoing interface list:
vlan1024 (1)
(192.168.77.3, 233.1.1.3), uptime 00:01:04, stat expires 00:03:24
Owner PIM-SM, Flags: TF
Incoming interface: vlan400
Outgoing interface list:
vlan1024 (1)
switch#
```

show ip mvif

Command

```
show ip mvif [<if-name>]
```

Mode

Normal mode/privileged mode.

Parameters

if-name: the name of the interface, specifying the interface to be displayed.
Default: information about all interfaces is displayed.

Description

The show ip mvif command is used to display the multicast interface index, update time, interface address, and other interface attributes.

Examples

Display current multicast interface information.

```
switch#show ip mvif
Interface Vif Owner TTL Local Remote Uptime
Idx Module Address Address
vlan1024 0 PIM-SM 1 192.168.8.2 0.0.0.0 00:15:27
Register 1 1 192.168.8.2 0.0.0.0 00:15:27
vlan400 2 PIM-SM 1 192.168.77.2 0.0.0.0 00:06:28
switch#
```

show ip pim sparse-mode bsr-router

Command

```
show ip pim sparse-mode bsr-router
```

Mode

Normal mode/privileged mode.

Parameters

None

Description

The show ip pim sparse-mode bsr-router command is used to display information about BSR routers in sparse mode.

Examples

Display when BSR router information.

```
switch#show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.100.1
Uptime: 00:00:11, BSR Priority: 0, Hash mask length: 10
Expires: 00:01:59
Role: Candidate BSR
State: Pending BSR
Candidate RP: 192.168.100.1(vlan100)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:40
switch#
```

show ip pim sparse-mode interface

Command

```
show ip pim sparse-mode interface [detail]
```

Mode

Normal mode/privileged mode.

Parameters

Default: display summary information for the PIM-SM interface.
detail: Displays the detailed information of the PIM-SM interface.

Description

The show ip pim sparse-mode interface command is used to display the information of PIM-SM enabled interfaces, including the interface name, interface address, neighbor and DR status, etc.

Examples

Display system start-up PIM-SM interface information.

```
switch#show ip pim sparse-mode interface detail
vlan11 (vif 2):
Address 192.168.11.4, DR 192.168.11.4
Hello period 30 seconds, Next Hello in 20 seconds
Triggered Hello period 5 seconds
Neighbors:
192.168.11.3
switch#
```

Display summary information for the PIM-SM interface.

```
switch#show ip pim sparse-mode interface
Address Interface VIFindex Ver/ Nbr DR DR
ode Count Prior
192.168.11.4 vlan11 2 v2/S 1 1 192.168.11.4
switch#
```

show ip pim sparse-mode local-members

Command

```
show ip pim sparse-mode local-members [ifname]
```

Mode

Normal mode/privileged mode.

Parameters

Default: displaying information about all current PIM-SM local members of the system.
ifname: Specify the interface name and display the local members associated with the interface.

Description

The show ip pim sparse-mode local-members command is used to display the information of the interfaces on which the system has started PIM-SM, including interface name, interface address, neighbor and DR status, etc.

Examples

Display system local membership information.

```
switch#show ip pim sparse-mode local-members
PIM Local membership information
vlan1024:
vlan400:
switch#
```

show ip pim sparse-mode mroute

Command

```
show ip pim sparse-mode mroute
```

Mode

Normal mode/privileged mode.

Parameters

None.

Description

The show ip pim sparse-mode mroute command is used to display multicast routing information of PIM-SM, including various types of multicast routing entries such as (*,*,RP), (*,G), (S,G), (S,G,RPT).

Examples

Display the system's PIM-SM multicast routing information.

```
switch#show ip pim sp mrout
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 2
(S,G,rpt) Entries: 1
FCR Entries: 0
(*, 233.1.1.1)
RP: 192.168.8.4
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
Local: vlan93
Joined:
Asserted:
FCR:
(192.168.8.2, 233.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local:
Joined: reg
Asserted:
Outgoing: vlan93 reg
(192.168.8.2, 233.1.1.1, rpt)
RP: 192.168.8.4
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
Local:
Pruned:
Outgoing: vlan93
switch#
```

show ip pim sparse-mode neighbor

Command

```
show ip pim sparse-mode neighbor [detail]
```

Mode

Normal mode/privileged mode.

Parameters

Default: Display the neighbor summary information by default.
detail: Displays detailed information about the neighbor.

Description

The show ip pim sparse-mode neighbor command is used to display PIM-SM multicast neighbor information, including the neighbor ip address, discovery time and timeout time, local interface connected to the neighbor, neighbor priority, and other information.

Examples

Display the system's PIM-SM multicast routing information.

```
switch#show ip pim sparse-mode neighbor
Neighbor Interface Uptime/Expires Ver DR Priority/Mode
Address
192.168.11.3 vlan11 01d03h39m/00:01:44 v2 N /
switch#
```

show ip pim sparse-mode nexthop

Command

```
show ip pim sparse-mode nexthop
```

Mode

Normal mode/privileged mode.

Parameters

None.

Description

The show ip pim sparse-mode nexthop command is used to display the next-hop address calculated by the PIM-SM for RPF.

Examples

Display next-hop information for multicast routes in the current system.

```
switch#show ip pim sp nex
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination Type Nexthop Nexthop Nexthop Nexthop Nexthop Metric Pref Refcnt
Num Addr Ifindex Name
_____
192.168.8.2 . .S. 1 0.0.0.0 4 0 0 4
192.168.10.3 .R..  1 192.168.101.3 7 2 120 8
switch#
```

show ip pim sparse-mode rp

Command

```
show ip pim sparse-mode rp <mapping>
```

Mode

Normal mode/privileged mode.

Parameters
mapping: mapping of RPs to groups.

Description
The show ip pim sparse-mode rp mapping command is used to display the current RP-to-group mapping relationship in the PIM-SM, including the RP address, the group mapped by the RP, the uptime, and so on.

Examples
Display the current system RP mapping relationship.

```
switch#show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
RP: 192.168.11.4
Uptime: 01d06h33m
switch#
```

show ip pim sparse-mode rp-hash

Command

```
show ip pim sparse-mode rp-hash <grp-address>
```

Mode
Normal mode/privileged mode.

Parameters
grp-address: Specify the group address.

Description
The show ip pim sparse-mode rp-hash command is used to display the RPs mapped by the hash algorithm for the specified group.

Examples
Display the RP selection for group 234.1.1.1 in the current system.

```
switch#show ip pim sparse-mode rp-hash 234.1.1.1
RP: 192.168.11.4
switch#
```

Diagnostic and debugging commands

debug pim sparse-mode

Command

```
debug pim spare-mode
no debug pim sparse-mode
```

Mode
Privilege mode.

Parameters
None.

Description
The debug pim sparse-mode command is used to turn on all debug switches related to PIM-SM to be able to output debug information in the terminal.
The no debug pim sparse-mode command is used to turn off the debug switch of the PIM-SM.

Examples
Turn on the system's PIM-SM debug switch.

```
switch#debug pim sparse-mode
switch#show debugging pim sparse-mode
```

```
PIM-SM debugging status:
PIM event debugging is on
PIM MFC debugging is on
PIM state debugging is on
PIM packet debugging is on
PIM Hello HT timer debugging is on
PIM Hello NLT timer debugging is on
PIM Hello THT timer debugging is on
PIM Join/Prune JT timer debugging is on
PIM Join/Pune ET timer debugging is on
PIM Join/Prune PPT timer debugging is on
PIM Join/Prune KAT timer debugging is on
PIM Join/Prune OT timer debugging is on
PIM Assert AT timer debugging is on
PIM Register RST timer debugging is on
PIM Bootstrap BST timer debugging is on
PIM Bootstrap CRP timer debugging is on
PIM mib debugging is on
PIM nsm debugging is on
PIM nexthop debugging is on
switch#
```

debug pim sparese-mode all

Command

```
debug pim spare-mode all
no debug pim sparse-mode all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug pim sparse-mode all command is used to turn on all debug switches related to PIM-SM and to be able to output debug information of all PIM-SM in the terminal.
The no debug pim sparse-mode all command is used to turn off all debug switches of the PIM-SM.

Examples

Turn on all PIM-SM debug switches in the system.

```
switch#debug pim sparse-mode all
switch#
```

debug pim sparse-mode event

Command

```
debug pim spare-mode events
no debug pim sparse-mode events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug pim sparse-mode events command is used to turn on the event debugging switch of PIM-SM, which can output event debugging information in the terminal.
The no debug pim sparse-mode events command is used to turn off the event debug switch of PIM-SM.

Examples

Turn on the PIM-SM event debug switch.

```
switch#debug pim sparse-mode events
switch#log display
switch#
2006/10/26 15:11:39 Informational: PIM-SM: WholePkt message: src 192.168.8.2 for 233.1.1.2 vif 1
2006/10/26 15:11:40 Informational: PIM-SM: Hello Timer expired on vlan100
2006/10/26 15:11:40 Informational: PIM-SM: Restarting Hello Timer on vlan100 with 30 secs timeout
2006/10/26 15:11:40 Informational: PIM-SM: Stopping Triggered Hello Timer on vlan100
switch#no log display
switch#
```

debug pim sparse-mode mfc

Command

```
debug pim spare-mode mfc
no debug pim sparse-mode mfc
```

Mode

Privilege mode.

Parameters

None.

Description

The debug pim sparse-mode mfc command is used to turn on the MFC debug switch of PIM-SM to be able to output debug information related to multicast route writing and deletion in the terminal.
The no debug pim sparse-mode mfc command is used to turn off the MFC debug switch of the PIM-SM.

Examples

Turn on the MFC debug switch of PIM-SM.

```
switch#debug pim sparse-mode mfc
switch#show debugging pim sparse-mode
PIM-SM debugging status:
PIM MFC debugging is on
switch#log display
switch#
2006/10/26 15:16:51 Informational: PIM-SM: MFC add message to MRIB for (192.168.8.2, 233.1.1.2) iif:2
olist:0x00000002 succeeded
2006/10/26 15:16:51 Informational: PIM-SM: MFC add message to MRIB for (192.168.8.2, 233.1.1.1) iif:2
olist:0x00000002 succeeded
2006/10/26 15:16:51 Informational: PIM-SM: MRT ADD notification for (192.168.8.2, 233.1.1.2) status:
14 msg_id: 312
2006/10/26 15:16:51 Informational: PIM-SM: MRIB MRT add for (192.168.8.2, 233.1.1.2) MRT succeeded
2006/10/26 15:16:51 Informational: PIM-SM: MRT ADD notification for (192.168.8.2, 233.1.1.1) status:
14 msg_id: 313
2006/10/26 15:16:51 Informational: PIM-SM: MRIB MRT add for (192.168.8.2, 233.1.1.1) MRT succeeded
switch#no log display
```

debug pim sparse-mode mib

Command

```
debug pim spare-mode mib
no debug pim sparse-mode mib
```

Mode

Privilege mode.

Parameters

None.

Description
debug pim sparse-mode mib to turn on the mib off of PIM-SM and be able to output debugging information in the terminal that the pim multicast route has changed.
no debug pim sparse-mode mib to disable the mib debug switch of PIM-SM.

Examples
```
switch#debug pim sparse-mode mib
switch#
```

debug pim sparse-mode nexthop

Command
```
debug pim spare-mode nexthop
no debug pim sparse-mode nexthop
```

Mode
Privilege mode.

Parameters
None.

Description
debug pim sparse-mode nexthop to turn on debugging information related to the next hop of multicast routes.
no debug pim sparse-mode nexthop to turn off multicast next-hop debug information.

Examples
Turn on the next-hop check debug switch to display multicast next-hop related information
```
switch#debug pim sparse-mode nexthop
switch#show debugging pim sparse-mode
PIM-SM debugging status:
PIM nexthop debugging is on
switch#log display
switch#
2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.4: Increment refcnt 3
2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.2: Increment refcnt 3
2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.4: Increment refcnt 4
switch#no log display
```

debug pim sparse-mode packets

Command
```
debug pim spare-mode packets [recv | send]
no debug pim sparse-mode packets [rec | send]
```

Mode
Privilege mode.

Parameters
recv: the received message.
send: The message sent.
By default both receive and send are turned on.

Description
The debug pim sparse-mode packets command is used to turn on the PIM-SM message debugging switch to be able to output information about received and sent pim protocol messages at the terminal.
no debug pim sparse-mode packets to disable the PIM-SM packet debug switch.

Examples
Turn on the pim-sm receive message debug switch
```
switch#debug pim sp packets recv
switch#show debugging pim sparse-mode
```

```
PIM-SM debugging status:
PIM packet receive debugging is on
switch#
```

debug pim sparse-mode state

Command

```
debug pim spare-mode state
no debug pim sparse-mode state
```

Mode

Privilege mode.

Parameters

None.

Description

The debug pim sparse-mode state command is used to turn on the multicast routing state debug switch.
no debug pim sparse-mode state to turn off the multicast routing state debug switch.

Examples

Turn on the pim-sm route state debug switch to see the state change of multicast routes when members leave

```
switch#debug pim sparse-mode state
switch#log dis
switch#
2006/10/26 17:01:16 Informational: PIM-SM: US (*, 233.1.1.1): JOINED to NOT JOINED, JoinDesired =>
FALSE
2006/10/26 17:01:16 Informational: PIM-SM: US (192.168.8.2, 233.1.1.1, rpt): NOT PRUNED to RPT NOT
JOINED, RPTJoinDesired(G)=>FALSE
switch#
```

debug pim sparse-mode timer

Command

```
debug pim spare-mode timer [assert [at] | bsr [bst | crp] | hello [ht | nlt | tht] | joinprune [et |
jt | kat | ot | ppt] | register [rst]]
no debug pim sparse-mode timer [assert [at] | bsr [bst | crp] | hello [ht | nlt | tht] | joinprune
[et | jt | kat | ot | ppt] | register [rst]]
```

Mode

Privilege mode.

Parameters

assert [at]: assert timer.
bsr [bst | crp]: bootstrap timer and candidate rp timer for bootstrap routers.
hello [ht | nlt | tht]: hello timer, contains hello timer, neighbor expiration timer and hello trigger timer.
joinprune [et | jt | kat | ot | ppt]: joinprune timer, including timeout timer, joinprune timer, keep-alive timer, veto timer and prune suppression timer.
register [rst]: Register the timer.

Description

The debug pim spare-mode timer command is used to turn on the debug switch for the specified timer.
The no debug pim sparse-mode timer command is used to turn off the debug switch for the specified timer.

Examples

```
#Turn on the debug switch for the pim-sm hello message timer
switch#debug pim sparse-mode timer hello
switch#show debugging pim sparse-mode
PIM-SM debugging status:
PIM Hello HT timer debugging is on
```

```
PIM Hello NLT timer debugging is on
PIM Hello THT timer debugging is on
switch#
```

CHAPTER 27

RIP command

Configuration commands

default-information originate

Command

```
default-information originate
no default-information originate
```

Mode

rip configuration mode

Parameters

None

Description

The default-information originate command is used to start the rip protocol to generate default routes and spread them to other routers.
The no default-information originate command is used to disable the local rip from generating default routes.

Examples

```
#startrip to generate default rip routes
switch(config-router)#default-information originate
switch(config-router)#
```

default-metric

Command

```
default-metric <metric>
no default-metric [<metric>]
```

Mode

rip configuration mode

Parameters

metric: the default spend of the introduced route, takes a value in the range of 1 to 16, the default is 1.

Description

The default-metric command is used to specify the default spend when rip introduces a route.
The no default-metric command is used to restore the default value of the introduced route and restore the metric value to the default value.

Examples

Configure rip introduction route with a default value of 7

```
switch(config-router)#default-metric 7
switch(config-router)#
```

distance

Command

```
distance <distance-value>
no distance [<distance-value>]
```

Mode
rip configuration mode

Parameters
distance-value: Specifies the administrative distance (or protocol priority) value of the rip route, in the range of 1 to 255. the default value is 130.

Description
The distance command is used to specify the administrative distance (protocol priority) of the rip route.
The no distance command is used to remove the configuration of the administrative distance and restore it to the default value.

Examples
Configure rip with an administrative distance of 100

```
switch(config-router)#distance 100
switch(config-router)#
```

distribute-list

Command

```
distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
no distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
```

Mode
rip configuration mode.

Parameters
acl-name: the name of the access control list.
prefix-list: the name of the prefix list.
in: Use filtering on the incoming interface.
out: Use filtering on the outgoing interface.
if-name: Specify the interface to use the filtering function, the default is all interfaces that start RIP protocol.

Description
The distribute-list command is used to configure the use of access control lists and prefix lists to filter routes on input and output interfaces.
The no distribute-list command is used to cancel the configuration of route filtering.

Examples
Configure incoming routes to be filtered on interface vlan3 using an access control list named list123

```
switch(config-router)#distribute-list list123 in vlan3
switch(config-router)#
```

ip rip authentication

Command

```
ip rip authentication {mode <mode> | key-chain <key-chain> | string <string>}
no ip rip authentication [mode <mode> | key-chain <key-chain> | string <string>]
```

Mode
Interface configuration mode.

Parameters
mode: mode of authentication, takes the value of md5 mode and text (simple text mode).
key-chain : key-chainming, configured to call the authentication code configured in the corresponding key-chain.
string: Authentication code, in string form, no more than 16 characters.

Description
The ip rip authentication command is used to enable the authentication of RIP messages on an interface and configure the related parameters.

The no ip rip authentication command is used to cancel the authentication function of the interface for RIP messages or to modify and delete related parameters.

Examples

Configure interface vlan55 to use authentication when running the RIP protocol with md5 as the authentication method and pass123 as the authentication password.

```
switch(config-vlan55)#ip rip authentication mode md5
switch(config-vlan55)#ip rip authentication string pass123
switch(config-vlan55)#
```

ip rip metric

Command

```
ip rip metric <metric>
no ip rip metric [<metric>]
```

Mode

Interface configuration mode.

Parameters

metric: metric value, the value range is 1 to 16.

Description

The ip rip metric command is used to configure the increment of the metric value when the interface receives RIP routes, which is 1 by default.
The no ip rip metric command is used to cancel the configuration of the incoming interface metric increment and revert to the default value.

Examples

Configure the metric value to increase by 3 when sending RIP routes on interface vlan55.

```
switch(config-vlan55)#ip rip metric 3
switch(config-vlan55)#
```

ip rip receive version

Command

```
ip rip receive version <version>
no ip rip receive version [<version>]
```

Mode

Interface configuration mode.

Parameters

version: The version of RIP messages allowed to be received. The value is 1, 2 or 1 2, i.e. both. The default is 2.

Description

The ip rip receive version command is used to configure the version of RIP packets received by the interface.
The no ip rip receive version command is used to restore the version of RIP messages received by the interface to the default value.

Examples

Configure interface vlan55 to allow receiving RIP packets with version number 1.

```
switch(config-vlan55)#ip rip receive version 1
switch(config-vlan55)#
```

ip rip receive-packet

Command

```
ip rip receive-packet
no ip rip receive-packet
```

Mode
Interface configuration mode.

Parameters
None.

Description
The ip rip receive-packet command is used to enable the interface to receive RIP packets.
The no ip rip receive-packet command is used to configure the interface not to receive RIP packets.

Examples
Configure interface vlan55 to allow receiving RIP packets.
```
switch(config-vlan55)# ip rip receive-packet
switch(config-vlan55)#
```
Configure interface vlan55 to not receive RIP packets
```
switch(config-vlan55)#no ip rip receive-packet
switch(config-vlan55)#
```

ip rip send version

Command
```
ip rip send version <version>
no ip rip send version [<version>]
```

Mode
Interface configuration mode.

Parameters
version: The version of RIP messages allowed to be sent, takes the value of 1 or 2. The default is 2.

Description
The ip rip send version command is used to configure the version of RIP messages sent by the interface.
The no ip rip send version command is used to restore the version of RIP messages sent by the interface to the default value.

Examples
Configure interface vlan55 to allow RIP messages with version number 1 to be sent on it.
```
switch(config-vlan55)#ip rip send version 1
switch(config-vlan55)#
```

ip rip send-packet

Command
```
ip rip send-packet
no ip rip send-packet
```

Mode
Interface configuration mode.

Parameters
None.

Description
The ip rip send-packet command is used to enable the interface to send RIP packets.
The no ip rip send-packet command is used to configure the interface not to send RIP packets.

Examples
Configure interface vlan55 to allow RIP packets to be sent on it.
```
switch(config-vlan55)# ip rip send-packet
switch(config-vlan55)#
```
Configure interface vlan55 to not send RIP packets
```
switch(config-vlan55)#no ip rip send-packet
```

```
switch(config-vlan55)#
```

ip rip split-horizon

Command

```
ip rip split-horizon [poisoned]
no ip rip split-horizon
```

Mode

Interface configuration mode.

Parameters

poisoned: horizontal splitting method with toxicity reversal.

Description

The ip rip split-horizon command is used to enable the horizontal splitting feature on an interface. The default is horizontal splitting with toxicity reversal.
The no ip rip split-horizon command is used to configure the horizontal split feature not to be used on an interface.

Examples

Configure horizontal segmentation with toxicity reversal to be enabled on interface vlan55.

```
switch(config-vlan55)# ip rip split-horizon poisoned
switch(config-vlan55)#
```

maximum-prefix

Command

```
maximum-prefix <max-num> [<waring-num>]
no maximum-prefix [<max-num>] [<waring-num>]
```

Mode

rip configuration mode.

Parameters

max-num: the maximum number of RIP routes, the value range is 1 to 65535.
waring-num: The percentage of routing alarms issued, the value range is 1 to 100.

Description

The maximum-prefix command is used to configure the routing table capacity and alarm tolerance.
The no maximum-prefix command is used to cancel the capacity limit and alarm configuration for the routing table.

Examples

Configure RIP routes to a maximum of 1000 and issue an alarm when 60% is reached

```
switch(config-router)#maximum-prefix 1000 60
switch(config-router)#
```

neighbor

Command

```
neighbor <neighbor-address>
no neighbor <neighbor-address>
```

Mode

rip configuration mode.

Parameters

neigubor-address: ip address of the neighbor, in dotted decimal format.

Description

The neighbor command specifies a neighbor for RIP on a non-broadcast network.
The no neighbor command cancels the specified neighbor.

Examples

Designated neighbor 10.80.50.111

```
switch(config-router)#neighbor 10.80.50.111
switch(config-router)#
```

network

Command

```
network {<ip-prefix>/<mask-length> | < ip-prefix ><mask>}
no network {<ip-prefix>/<mask-length> | < ip-prefix ><mask>}
```

Mode

rip configuration mode.

Parameters

ip-prefix: ip address prefix.
mask-length: the length of the decimal mask.
mask: 32-bit dot-division decimal mask.

Description

The network command is used to enable a subnet to run the RIP protocol.
The no network command is used to disable a subnet from enabling the RIP protocol.

Examples

Specify subnet 192.168.1.0/24 to run RIP protocol

```
switch(config-router)#network 192.168.1.0/24
switch(config-router)#
```

offset-list

Command

```
offset-list <acl-name> {in | out} <metric> [<if-name>]
no offset-list <acl-name> {in | out} <metric> [<if-name>]
```

Mode

rip configuration mode.

Parameters

acl-name: the name of the invoked access control list.
in: Apply on the in interface.
out: Apply on the outgoing interface.
metric: the offset of the route metric value.
if-name: The interface to which the rule is applied, default is all interfaces.

Description

The offset-list command is used to configure RIP to add a certain offset value to the incoming or outgoing routes of an interface through ACL filtering.
The nooffset-list command is used to cancel the offset increment configuration for a specific route.

Examples

```
#Increase the metric value on vlan3 for routes filtered by the access control list named "list123" by
3
switch(config-router)#offset-list list123 out 3 vlan3
switch(config-router)#
```

passive-interface

Command

```
passive-interface <if-name>
no passive-interface <if-name>
```

Mode
rip configuration mode.

Parameters
if-name: Specifies the interface.

Description
The passive-interface command is used to configure the interface as a passive interface. After configuration, the interface can receive RIP messages, but cannot send RIP messages.
The no passive-interface command is used to restore the interface to the transceiver state.

Examples
Configure interface vlan3 as a passive interface

```
switch(config-router)#passive-interface vlan3
switch(config-router)#
```

recv-buffer-size

Command

```
recv-buffer-size <buffer-size>
no recv-buffer-size [<buffer-size>]
```

Mode
rip configuration mode.

Parameters
buffer-size: Receive buffer size value, ranging from 8192 to 2147483647.

Description
The recv-buffer-size command is used to configure the size of the RIP message receive buffer.
The no recv-buffer-size command is used to unspecify the size of the RIP receive buffer

Examples
Configure the receive buffer size to 102400

```
switch(config-router)# recv-buffer-size 102400
switch(config-router)#
```

redistribute

Command

```
redistribute <protocol> [metric <metric>] [route-map <route-map>]
no redistribute <protocol> [metric <metric>] [route-map <route-map>]
```

Mode
rip configuration mode.

Parameters
protocol:The type of routing protocol to be introduced into RIP such as is-is, ospf, bgp, static, connect, etc.
metric: Specifies the metric value when the route is introduced.
route-map: the name of the route-map to be referenced when introducing routes.

Description
redistribute is used to introduce routes from other protocols into RIP.
no redistribute is used to cancel the introduction of routes to other protocols. By default, no redistribution is done.

Examples

```
#Introduce directly connected routes into the RIP routing table, and specify the metric value of the
introduced routes as 9 through the route-map rule "list123" rule.
switch(config-router)#redistribute connected metric 9 route-map list123
switch(config-router)#
```

route

Command

```
route <network>/<mask-length>
no route <network>/<mask-length>
```

Mode

rip configuration mode.

Parameters

network: the destination network of the route.
mask-length: the length of the mask of the destination network.

Description

The route command is used to add a static route to the RIP routing table and then propagate the route within the RIP domain.
The no route command is used to cancel a static route that is added to RIP.

Examples

```
#Add a static route to the destination network 200.1.1.0/24 to the RIP routing table
switch(config-router)# route 200.1.1.0/24
switch(config-router)#
```

router rip

Command

```
router rip
no router rip
```

Mode

Global configuration mode

Parameters

None

Description

The router rip command is used to start the rip protocol and enter rip configuration mode.
The no router rip command is used to shut down the rip protocol and remove the configuration.

Examples

```
#boot and enter rip configuration mode
switch(config)#router rip
switch(config-router)#
```

timers

Command

```
timers basic <update-interval><dead-interval><garbage-interval>
no timers basic
```

Mode

rip configuration mode.

Parameters

update-interval: The time interval for sending RIP periodic update messages. The default is 30 seconds.
dead-interval: The wait time for RIP routes that are set to unavailable that do not get updated. The default is 180 seconds.
garbage-interval: The time interval after which a route from RIP is set to unavailable for complete removal from the routing table. The default is 120 seconds.

Description
The timers basic command is used to configure the timer values associated with RIP.
The no timers basic command is used to restore the RIP timers to their default values.

Examples
Configure the RIP protocol to have a periodic update time of 20 seconds, a death time of 100 seconds, and a garbage collection time of 60 seconds.

```
switch(config-router)#timers basic 20 100 60
switch(config-router)#
```

version

Command

```
version <version>
no version [<version>]
```

Mode
rip configuration mode.

Parameters
version: the version of RIP, the range of values: 1 to 2.

Description
The version command is used to specify the version of the RIP protocol, and the default value is 2.
The no version command is used to revert to the system default version.

Examples
Configure the version of RIP protocol to version 1.

```
switch(config-router)#version 1
switch(config-router)#
```

View command

show ip rip

Command

```
show ip rip [database[count] | interface [<if-name>]]
```

Mode
Privilege mode / Normal mode.

Parameters
Default: Display information about the current system rip.
database: View the rip routing information database.
count: displays the number of entries in the rip routing information database.
interface: View information about the interface where the rip protocol is enabled.
if-name: View rip-related information on the specified interface

Description
The show ip rip command is used to display the current rip information.

Examples
Display the current rip configuration on interface vlan51.

```
switch#show ip rip interface vlan51
vlan51 is up, line protocol is up
Routing Protocol: RIP
Receive RIP packets
Send RIP packets
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
```

```
IP interface address:
172.20.6.2/24
switch#
```

show ip route rip

Command

```
show ip route rip [count]
```

Mode

Privilege mode / Normal mode.

Parameters

Default: Displays the currently active rip routes.
count: Shows the number of currently active rip routes.

Description

The show ip route rip command is used to display information about the currently active rip routes.

Examples

Show the currently active rip routes.

```
switch#show ip route rip
R 1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
R 1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
R 1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
switch#
```

Displays the number of currently active rip routes.

```
switch#show ip rout rip count
total routes: 3
switch#
```

show running rip

Command

```
show running rip
```

Mode

Privilege mode / Normal mode.

Parameters

None.

Description

The show running rip command is used to display the current RIP configuration.

Examples

Display the current rip configuration.

```
switch#show running-config rip
!
router rip
network 172.20.13.0/24
network 172.20.14.0/24
!
switch#
```

Debugging commands

debug rip

Command

```
debug rip
no debug rip
```

Mode

Privilege mode.

Parameters

None.

Description

The debug rip command is used to turn on the debug switch for the current rip, enabling the user to see the negotiation process and the messages sent and received by the rip.
The no debug rip command is used to turn off the debug switch for rip.

Examples

Turn on the debug switch for rip.

```
switch#debug rip
switch#
```

debug rip all

Command

```
debug rip all
no debug rip all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug rip all command is used to turn on all rip-related debug switches so that users can see the negotiation process and the messages sent and received by the rip.
The no debug rip all command is used to turn off all rip-related debug switches.

Examples

Turn on all rip-related debug switches.

```
switch#debug rip all
switch#
```

debug rip events

Command

```
debug rip events
no debug rip events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug rip events command is used to turn on the rip's event debug switch, enabling the user to see the rip's negotiation process.

The no debug rip events command is used to turn off the event debug switch for rip.

Examples

Turn on rip's event debugging switch.

```
switch#debug rip events
switch#
```

debug rip packet

Command

```
debug rip packet [recv | send] [detail]
no debug rip packet [recv | send] [detail]
```

Mode

Privilege mode.

Parameters

recv: Turn on the receive message debug switch.
send: Turn on the send message debug switch.
detail: Turn on the detail debug switch for rip messages.

Description

The debug rip packet command is used to turn on the rip packet debug switch so that users can see how rip packets are sent and received.
The no debug rip packet command is used to turn off the rip packet debug switch.

Examples

Turn on rip's receive message details debug switch.

```
switch#debug rip packet recv detail
switch#
```

CHAPTER 28

RIPng command

Configuration commands

router ipv6 rip

Command

```
router ipv6 rip
no router ipv6 rip
```

Mode

Global configuration mode

Parameters

None

Description

The router ipv6 rip command is used to start the RIPng protocol and enter RIPng configuration mode.
The no router ipv6 rip command is used to shut down the RIPng protocol and remove the configuration.

Examples

```
#boot and enter RIPng configuration mode
switch(config)#router ipv6 rip
switch(config-router)#
```

ipv6 router rip

Command

```
ipv6 routerrip
no ipv6 router rip
```

Mode

Interface configuration mode

Parameters

None

Description

The ipv6 router rip command is used to start the RIPng protocol for an interface.
The no ripv6 router rip command is used to turn off the RIPng protocol for the interface.

Examples

Start the RIPng protocol for interface vlan1.

```
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#switch(config-router)#
```

ipv6 rip split-horizon

Command

```
ipv6 rip split-horizon [poisoned]
no ipv6 rip split-horizon
```

Mode

Interface configuration mode.

Parameters
poisoned: horizontal splitting method with toxicity reversal.

Description
The Ipv6 rip split-horizon command is used to enable the horizontal split function on an interface. The default is horizontal splitting with toxicity reversal.
The no ipv6 rip split-horizon command is used to configure the horizontal split feature not to be used on an interface.

Examples
Configure horizontal segmentation with toxicity reversal to be enabled on interface vlan55.

```
switch(config-vlan55)# ipv6 rip split-horizon poisoned
switch(config-vlan55)#
```

timers

Command

```
timers basic <update-interval><dead-interval><garbage-interval>
no timers basic
```

Mode
RIPng configuration mode.

Parameters
update-interval: The time interval for sending RIPng periodic update messages. The default is 30 seconds.
dead-interval: The wait time for RIPng routes that have not been updated and are set to unavailable. The default is 180 seconds.
garbage-interval: The time interval after which a route from RIPng is set to unavailable for complete removal from the routing table. The default is 120 seconds.

Description
The timers basic command is used to configure the timer values associated with RIPng.
The no timers basic command is used to restore the RIPng timer to its default value.

Examples
Configure the RIPng protocol to have a periodic update time of 20 seconds, a death time of 100 seconds, and a garbage collection time of 60 seconds.

```
switch(config-router)#timers basic 20 100 60
switch(config-router)#
```

neighbor

Command

```
neighbor <neighbor-address><ifname>
no neighbor <neighbor-address>
```

Mode
RIPng configuration mode.

Parameters
neigubor-address: Link-local address of the neighbor.
ifname:neighbor's vlanif interface

Description
The neighbor command specifies a neighbor for RIPng on the network.
The no neighbor command cancels the specified neighbor.

Examples
Designated neighbor 10.80.50.111

```
switch(config-router)#neighbor 10.80.50.111
switch(config-router)#
```

aggregate-address

Command

```
aggregate-address<network>
no aggregate-address<network>
```

Mode

RIPng configuration mode.

Parameters

network: ipv6 address segment, format X:X::X:X/M.

Description

The aggregate-address command is used to specify the RIPng instance summary route, using the prefix/length form, to send summary routes and reduce the number of routes maintained in the routing table.
The no aggregate-address command is used to cancel the corresponding setting

Examples

```
#subroutes for summary 2006:4:5::/35
switch(config-router)#aggregate-address 2006:4:5::/35
switch(config-router)#
```

default-metric

Command

```
default-metric <metric>
no default-metric [<metric>]
```

Mode

RIPng configuration mode

Parameters

metric: the default spend of the introduced route, takes the value range of 1 to 16, the default is 1.

Description

The default-metric command is used to specify the default spend when RIPng introduces routes.
The no default-metric command is used to restore the default value of the introduced route and restore the metric value to the default value.

Examples

Configure RIPng to introduce routes with a default value of 7

```
switch(config-router)#default-metric 7
switch(config-router)#
```

default-information originate

Command

```
default-information originate
no default-information originate
```

Mode

RIPng configuration mode

Parameters

None

Description

The default-information originate command is used to start the rip protocol to generate default routes and spread them to other routers.
The no default-information originate command is used to disable the local rip from generating default routes.

Examples

Start RIPng to generate default RIPng routes

```
switch(config-router)#default-information originate
switch(config-router)#
```

distribute-list

Command

```
distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
no distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
```

Mode

RIPng configuration mode.

Parameters

acl-name: the name of the access control list.
prefix-list: the name of the prefix list.
in: Use filtering on the incoming interface.
out: Use filtering on the outgoing interface.
if-name: Specify the interface to use the filtering function, the default is all interfaces that start RIP protocol.

Description

The distribute-list command is used to configure the use of access control lists and prefix lists to filter routes on input and output interfaces.
The no distribute-list command is used to cancel the configuration of route filtering.

Examples

Configure incoming routes to be filtered on interface vlan3 using an access control list named list123

```
switch(config-router)#distribute-list list123 in vlan3
switch(config-router)#
```

offset-list

Command

```
offset-list <acl-name> {in | out} <metric> [<if-name>]
no offset-list <acl-name> {in | out} <metric> [<if-name>]
```

Mode

RIPng configuration mode.

Parameters

acl-name: the name of the invoked access control list.
in: Apply on the in interface.
out: Apply on the outgoing interface.
metric: the offset of the route metric value.
if-name: The interface to which the rule is applied, default is all interfaces.

Description

The offset-list command is used to configure RIPng to add a certain offset value to the incoming or outgoing routes of an interface through ACL filtering.
The nooffset-list command is used to cancel the offset increment configuration for a specific route.

Examples

```
#Increase the metric value on vlan3 for routes filtered by the access control list named "list123" by
3
switch(config-router)#offset-list list123 out 3 vlan3
switch(config-router)#
```

passive-interface

Command

```
passive-interface <if-name>
no passive-interface <if-name>
```

Mode

RIPng configuration mode.

Parameters

if-name: Specifies the interface.

Description

The passive-interface command is used to configure the interface as a passive interface. After configuration, the interface can receive RIPng messages, but cannot send RIPng messages.
The no passive-interface command is used to restore the interface to the transceiver state.

Examples

Configure interface vlan3 as a passive interface

```
switch(config-router)#passive-interface vlan3
switch(config-router)#
```

recv-buffer-size

Command

```
recv-buffer-size <buffer-size>
no recv-buffer-size [<buffer-size>]
```

Mode

RIPng configuration mode.

Parameters

buffer-size: Receive buffer size value, ranging from 8192 to 2147483647.

Description

The recv-buffer-size command is used to configure the size of the reception buffer for RIPng messages.
The no recv-buffer-size command is used to unspecify the size of the RIPng receive buffer

Examples

Configure the receive buffer size to 102400

```
switch(config-router)# recv-buffer-size 102400
switch(config-router)#
```

redistribute

Command

```
redistribute <protocol> [metric <metric>] [route-map <route-map>]
no redistribute <protocol> [metric <metric>] [route-map <route-map>]
```

Mode

RIPng configuration mode.

Parameters

protocol:The type of routing protocol that needs to be introduced into RIPng such as is-is, ospf, bgp, static, connect, etc.
metric: Specifies the metric value when the route is introduced.
route-map: the name of the route-map to be referenced when introducing routes.

Description

redistribute is used to introduce routes from other protocols into RIPng.
no redistribute is used to cancel the introduction of routes to other protocols. By default, no redistribution is done.

Examples

```
#Introduce directly connected routes into the RIPng routing table, and specify the metric value of
the introduced routes as 9 by the route-map rule "list123" rule.
switch(config-router)#redistribute connected metric 9 route-map list123
switch(config-router)#
```

route

Command

```
route <network>/<mask-length>
no route <network>/<mask-length>
```

Mode

RIPng configuration mode.

Parameters

network: the destination network of the route, in ipv6 address format.
mask-length: the length of the mask of the destination network.

Description

The route command is used to add a static route to the RIPng routing table and then propagate the route within the RIPng domain.
The no route command is used to cancel a static route that is added to RIPng.

Examples

```
#Add a static route to the destination network 3ffe:506::/64 to the RIPng routing table
switch(config-router)# route 3ffe:506::/64
switch(config-router)#
```

View command

show ipv6 rip

Command

```
show ipv6 rip [database| interface [<if-name>]]
```

Mode

Privilege mode / Normal mode.

Parameters

Default: Display information about the current system RIPng.
database: View the RIPng routing information database.
interface: View information about the interface on which the RIPng protocol is enabled.
if-name: View the RIPng related information on the specified interface

Description

The show ipv6 rip command is used to display the current RIPng information.

Examples

Display the current RIPng configuration on interface vlan1.

```
switch#show ipv6 rip interface vlan1
```

show ipv6 route rip

Command

```
show ipv6 route rip
```

Mode

Privilege mode / Normal mode.

Parameters
None.

Description
The show ipv6 route rip command is used to display information about the currently active RIPng routes.

Examples
Display the currently active RIPng routes.

```
Switch#show ipv6 route rip
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
Timers: Uptime
R 3ffe:507::/64 [120/2] via fe80::2a7:c1ff:fed1:5581, vlan1, 00:04:42
Switch#
```

Debugging commands

debug ipv6 rip

Command

```
debug ipv6 rip
no debug ipv6 rip
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ipv6 rip command is used to turn on the debug switch for the current RIPng so that users can see the negotiation process and the messages sent and received by RIPng.
The no debug ipv6 rip command is used to turn off the debug switch for RIPng.

Examples
Turn on the debug switch for RIPng.

```
switch#debug ipv6 rip
switch#
```

debug ipv6 rip all

Command

```
debug ipv6 rip all
no debug ipv6 rip all
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ipv6 rip all command is used to turn on all RIPng-related debug switches so that users can see the negotiation process and the messages sent and received by RIPng.
The no debug ipv6 rip all command is used to turn off all RIPng-related debug switches.

Examples
Turn on all debug switches related to RIPng.

```
switch#debug ipv6 rip all
switch#
```

debug ipv6 rip events

Command

```
debug ipv6 rip events
no debug ipv6 rip events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ipv6 rip events command is used to turn on the event debug switch for RIPng, enabling users to see the negotiation process of RIPng.
The no debug ipv6 rip events command is used to turn off the event debugging switch for RIPng.

Examples

Turn on the event debugging switch for RIPng.

```
switch#debug ipv6 rip events
switch#
```

debug ipv6 rip packet

Command

```
debug ipv6 rip packet [recv | send] [detail]
no debug ipv6 rip packet [recv | send] [detail]
```

Mode

Privilege mode.

Parameters

recv: Turn on the receive message debug switch.
send: Turn on the send message debug switch.
detail: Turn on the detail debug switch for RIPng messages.

Description

The debug ipv6 rip packet command is used to turn on the RIPng packet debugging switch to enable users to see how RIPng packets are sent and received.
The no debug ipv6 rip packet command is used to turn off the RIPng packet debug switch.

Examples

Turn on rip's receive message details debug switch.

```
switch#debug rip packet recv detail
switch#
```

CHAPTER 29

OSPF commands

Configuration commands

area authentication

Command

```
area <area-id> authentication [message-digest]
no area <area-id> authentication
```

Mode

ospf configuration mode.

Parameters

area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
message-digest: Specify to use MD5 ciphertext authentication. If there is no parameter, plaintext authentication is used.

Description

The area <area-id> authentication command is used to configure an area to use authentication and specify the authentication method.
The no area <area-id> authentication command is used to cancel the area authentication function.

Examples

Configure region 1 of ospf process 11 to use MD5 authentication.

```
switch(config-router)#area 1 authentication message-digest
switch(config-router)#
```

area default-cost

Command

```
area <area-id> default-cost <cost>
no area <area-id> default-cost
```

Mode

ospf configuration mode.

Parameters

area-id: ospf area id, can be expressed in decimal, the value range is 0~4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
cost: Routing splurge value, takes the value range 0 to 16777214.

Description

The area <area-id> default-cost command is used to configure the default cost of summary routes sent from the ABR to the stub area and the nssa area.
The no area <area-id> default-cost command is used to cancel the default spend configuration for an area and revert to the default value.

Examples

```
#Configure the default cost for area 1 to 224.
switch(config-router)#area 1 default-cost 224
switch(config-router)#
```

area filter-list

Command

```
area <area-id> filter-list {access <access-list> | prefix <prefix-list>} {in | out}
no area <area-id> filter-list {access <access-list> | prefix <prefix-list> } {in | out}
```

Mode

ospf configuration mode.

Parameters

area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
access access-list: the name of the access control list.
prefix prefix-list: the name of the address prefix list.
in: Specified as valid for the inbound direction.
out: specified as valid for the outgoing direction.

Description

The area <area-id> filter-list command is used to configure filters on the ABR, either using access list or prefix list to filter summary routes. in is the direction to be poured into this area, and out is the direction to be broadcast out from this area.
The no area <area-id> filter-list command is used to cancel the filtering of area summary routes on the ABR.

Examples

Configure the ABR of area 1 of ospf process 11 to filter incoming routes using a prefix list named list123 on.

```
switch(config-router)#area 1 filter-list prefix list123 in
switch(config-router)#
```

area nssa

Command

```
area <area-id> nssa [default-information-originate] [no-redistribution] [no-summary]
[translator-role]
no area <area-id> nssa [default-information-originate] [no-redistribution] [no-summary]
[translator-role]
```

Mode

ospf configuration mode.

Parameters

area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
default-information-originate: Generate a default route of type 7 to be sent to the nssa area.
no-redistribution: Specifies that the nssa area cannot be introduced using routes.
no-summary: Configure the ABR not to send summary type LSAs to the NSSA area.
translator-role: Specify the ABR for the nssa zone.

Description

The area <area-id> nssa command is used to configure an area as an nssa area, and can also specify related parameters.
The no area <area-id> nssa command is used to restore the area to a normal area or to remove the parameters of the nssa area.

Examples

Configure area 1 of ospf process 11 to be an nssa area, the router generates a default route of type 7, and the ABR does not spread summaryLSA into the nssa area.

```
switch(config-router)#area 1 nssa default-information-originate no-summary
switch(config-router)#
```

area range

Command

```
area <area-id> range <ip-prefix> [advertise | not-advertise]
no area <area-id> range <ip-prefix> [advertise | not-advertise]
```

Mode

ospf configuration mode.

Parameters

area-id: ospf area id, can be expressed in decimal, the value range is 0~4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
ip-prefix: The aggregated routing range, network/mask format.
advertise: Advertise the aggregated route after aggregation.
not-advertise: routes that are not advertised for aggregation.

Description

The area <area-id> range command is used to configure route aggregation or additional parameters within an area.
The no area <area-id> range command is used to cancel route aggregation for an area or remove additional parameters.

Examples

Configure area 1 of ospf process 11 for route aggregation and advertise the aggregated route.

```
switch(config-router)#area 1 range 1.1.1.1/8 advertise
switch(config-router)#
```

area shortcut

Command

```
area <area-id> shortcut [default | disable | enable]
no area <area-id> shortcut [default | disable | enable]
```

Mode

ospf configuration mode.

Parameters

area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
default: default mode.
disable: Disable.
enable: Forced.

Description

The area <area-id> shortcut command is used to configure the shortcut feature of an area, which, when enabled, allows data streams to pass through non-backbone areas at a small cost regardless of whether the ABR is connected to the backbone area.
The no area <area-id> shortcut command is used to cancel the shortcut configuration for an area.

Examples

Configure the shortcut function for area 1 of ospf process 11.

```
switch(config-router)#area 1 shortcut enable
switch(config-router)#
```

area stub

Command

```
area <area-id> stub [no-summary]
no area <area-id> stub [no-summary]
```

Mode
ospf configuration mode.

Parameters
area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
no-summary: Configure the ABR not to advertise summary routes to the stub area. By default, notification is allowed.

Description
The area <area-id> stub command is used to specify the area as the stub area.
The no area <area-id> stub command is used to unspecify an area as a stub area.

Examples
Configure area 1 of ospf process 11 as a stub area, without learning summary routes.

```
switch(config-router)#area 1 stub no-summary
switch(config-router)#
```

area virtual-link

Command

```
area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval
<hello-interval>] [ retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]
no area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval
<hello-interval>] [ retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]
```

Mode
ospf configuration mode.

Parameters
area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
neighbor-id: Router-id of the router on the opposite end of the virtual connection.
dead-interval: Configure the death time for router failure on a dummy connection. The default is 4 times the hello message period (40s).
hello-interval: Configure the time interval for hello messages to be sent on a virtual connection. The default is 10s.
retran-interval: Configures the message retransmission interval on a virtual connection. The default is 5s.
delay-interval: Configure the delay time for message transmission on a virtual connection. The default is 40s.

Description
The area <area-id> virtual-link command is used to configure a virtual connection and related parameters.
The no area <area-id> virtual-link command is used to remove the virtual link or restore the parameters on the virtual link to the default configuration.

Examples
Configure the virtual connection to neighbor 1.1.1.1 in area 1 of ospf process 11 with a hello interval of 5s.

```
switch(config-router)#area 1 virtual-link 1.1.1.1 hello-interval 5
switch(config-router)#
```

area virtual-link authentication

Command

```
area <area-id> virtual-link <neigubor-id> [authentication] [authentication-key <key-string>]
[message-digest] [message- digest-key <key-id> md5 <key-string>] [null]
no area <area-id> virtual-link <neigubor-id> [authentication] [authentication-key <key-string>]
[message-digest] [message -digest-key <key-id> md5 <key-string>] [null]
```

Mode
ospf configuration mode.

Parameters
neigubor-id: Router-id of the router on the opposite end of the virtual connection.
area-id: ospf area id, can be expressed in decimal, the value range is 0~4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
authentication: Configure the virtual connection to use the authentication feature.
authentication-key key-string: Configure the authentication word to use simple authentication.
message-digest: Configure the use of secret message authentication.
message-digest-key key-id md5 key-string: Configure the use of md5 secret message authentication and the id and authentication word of the authentication word.
null: Do not use the validation function.

Description
The area <area-id> virtual-link authentication command is used to configure the authentication function and related parameters for a virtual connection.
The no area <area-id> virtual-link authentication command is used to remove the authentication or authentication-related parameters on a virtual connection.

Examples
Configure ospf process 11 on area 1 to establish a virtual connection with neighbor 1.1.1.1 using simple text authentication.

```
switch(config-router)#area 1 virtual-link 1.1.1.1 authentication authentication-key pass123
switch(config-router)#
```

auto-cost reference-bandwidth

Command

```
auto-cost reference-bandwidth <bandwidth>
no auto-cost reference-bandwidth
```

Mode
ospf configuration mode.

Parameters
bandwidth: the reference bandwidth in Mbits/s, the range is 1 to 4294967, the default is 10000Mbits/s.

Description
The auto-cost reference-bandwidth command is used to configure the reference bandwidth value, and the ospf protocol calculates the spend of the route based on the configured value.
The no auto-cost reference-bandwidth command is used to remove the configuration of the reference bandwidth value and restore it to the default value.

Examples
Configure ospf process 11 with a reference bandwidth of 1000Mbits/s.

```
switch(config-router)#auto-cost reference-bandwidth 1000
switch(config-router)#
```

compatible rfc1583

Command

```
compatible rfc1583
no compatible rfc1583
```

Mode
ospf configuration mode.

Parameters
None.

Description
The compatible rfc1583 command is used to configure the local ospf protocol to be compatible with rfc1583.

The no compatible rfc1583 command is used to configure the local ospf to be incompatible with rfc1583.

Examples

Configure ospf process 11 to be compatible with rfc1583.

```
switch(config-router)#compatible rfc1583
switch(config-router)#
```

default-information originate

Command

```
default-information originate [always] [metric] [metric-type] [route-map]
no default-information originate [always] [metric] [metric-type] [route-map]
```

Mode

ospf configuration mode.

Parameters

always: always advertise the default route.
metric: The spend to notify the default route.
metric-type: The type of the notification default route, takes the value of 1 or 2, the default is 2.
route-map: Invoke the route-map rule when announcing the default route.

Description

The default-information originate command is used to configure the local router to generate a default ospf route and related parameters and notify the neighbors.
The no default-information originate command is used to cancel the generation of default routes or change the related parameters.

Examples

Configure ospf process 11 to generate a default route with a metric of 12.

```
switch(config-router)#default-information originate metric 12
switch(config-router)#
```

default-metric

Command

```
default-metric <metric>
no default-metric [<metric>]
```

Mode

ospf configuration mode.

Parameters

metric: the default spend of the introduced route, the value range is 0 to 16777214, the default is 1.

Description

The default-metric command is used to configure the default metric value of the route introduced by ospf.
The no default-metric command is used to restore the metric value of the introduced route to the default value.

Examples

Configure ospf process 11 to introduce routes with a default metric of 12.

```
switch(config-router)#default-metric 12
switch(config-router)#
```

distance

Command

```
distance {<distance> | ospf external <distance> | ospf inter-area <distance> | ospf intra-area
<distance>}
no distance {<distance> | ospf external <distance> | ospf inter-area <distance> | ospf intra-area
<distance>}
```

Mode
ospf configuration mode.

Parameters
distance: the administrative distance of the route, the value range is 1 to 255, the default is 110.
external: The external route obtained through route introduction.
inter-area: Inter-area routing.
intra-area: Intra-area routing.

Description
The distance command is used to configure the administrative distance of ospf routes.
The no distance command is used to restore the administrative distance of ospf routes to the default value.

Examples
Configure ospf routes with an administrative distance of 120.

```
switch(config-router)#distance 120
switch(config-router)#
```

distribute-list

Command

```
distribute-list <acl-list> out <protocol>
no distribute-list <acl-list> out <protocol>
```

Mode
ospf configuration mode.

Parameters
acl-list: the name of the access control list.
out: Filter when announcing routes to the outside.
protocol: Specifies the target protocol for the filtering implementation.

Description
The distribute-list command is used to configure the filtering of introduced routes when ospf advertises routes.
The no distribute-list command is used to cancel route filtering.

Examples
Configure ospf announcement routes to filter the introduced rip routes using an acl named list123.

```
switch(config-router)# distribute-list list123 out rip
switch(config-router)#
```

host

Command

```
host <host-address> area <area-id> [cost <cost>]
no host <host-address> area <area-id} [cost <cost>]
```

Mode
ospf configuration mode.

Parameters
host-address: host address, 32-bit dotted decimal.
area-id: area id, dotted decimal 0.0.0.0 to 255.255.255.255 or number 0 to 4294927695.
cost: Routing spend, takes the value range 0 to 65535.

Description
The host command is used to configure a host route within an area, which is broadcast out as a stub type link in the router lsa.
The no host command is used to cancel the host routing and related configuration.

Examples

Configure ospf 11 to advertise a host route to 172.20.1.1 in area 1 with a cost of 5.

```
switch(config-router)#host 172.20.1.1 area 1 cost 5
switch(config-router)#
```

ip ospf authentication

Command

```
ip ospf authentication [message-digest] [null]
no ip ospf authentication
```

Mode

Interface configuration mode.

Parameters

Default: Use simple text validation.
message-digest: use ciphertext authentication.
null: No validation is used.

Description

The ip ospf authentication command is used to configure the authentication mode of the configured interface.
The no ip ospf authentication command is used to cancel interface authentication.

Examples

Configure interface vlan5 to use simple text authentication.

```
switch(config-vlan5)#ip ospf authentication
switch(config-vlan5)
```

ip ospf authentication-key

Command

```
ip ospf authentication-key <key-string>
no ip ospf authentication-key
```

Mode

Interface configuration mode.

Parameters

key-string: the password for simple text authentication.

Description

The ip ospf authentication-key command is used to configure the password for simple text authentication.
The no ip ospf authentication-key command is used to remove the password for simple text authentication.

Examples

Configure interface vlan5 to use the simple text authentication password "pass123".

```
switch(config-vlan5)#ip ospf authentication-key pass123
switch(config-vlan5)
```

ip ospf cost

Command

```
ip ospf cost <cost>
no ip ospf cost
```

Mode

Interface configuration mode.

Parameters

cost: The link spend of the interface, the value range is 1 to 65535.

Description
The ip ospf cost command is used to configure the link spend of the interface, which is valid for outgoing interface routes.
The no ip ospf cost command is used to restore the link spend of an interface to the default value.

Examples
Configure the link spend for interface vlan5 to 23.
```
switch(config-vlan5)#ip ospf cost 23
switch(config-vlan5)
```

ip ospf database-filter

Command
```
ip ospf database-filter all out
no ip ospf database-filter
```

Mode
Interface configuration mode.

Parameters
all: All the routing information.
out: out direction blocked.

Description
The ip ospf database-filter command is used to configure an interface to block flooding.
The no ip ospf database-filter command is used to restore the flooding function of an interface.

Examples
Configure interface vlan5 not to send LSA information for ospf.
```
switch(config-vlan5)# ip ospf database-filter all out
switch(config-vlan5)
```

ip ospf dead-interval

Command
```
ip ospf dead-interval <interval>
no ip ospf dead-interval
```

Mode
Interface configuration mode.

Parameters
interval: the time of the dead timer on the interface, the value range is 1 to 65535, the default is 40 on the broadcast network, and the unit is seconds.

Description
The ip ospf dead-interval command is used to configure the dead timer value of an interface.
The no ip ospf dead-interval command is used to restore the interface dead timer to the default value.

Examples
Configure the ospf neighbor dead time on interface vlan5 to 20s.
```
switch(config-vlan5)# ip ospf dead-interval 20
switch(config-vlan5)
```

ip ospf disable all

Command
```
ip ospf disable all
no ip ospf disable all
```

Mode
Interface configuration mode.

Parameters
None.

Description
ip ospf disable disables all features of the interface and no longer processes packets; this command takes precedence over the network command. This command is valid only for Layer 3 interfaces.
The no ip ospf disable command is used to restore the ospf function of an interface.

Examples
Configure interface vlan5 to disable the ospf function on.

```
switch(config-vlan5)# ip ospf disable all
switch(config-vlan5)
```

ip ospf hello-interval

Command

```
ip ospf hello-interval <interval>
no ip ospf hello-interval
```

Mode
Interface configuration mode.

Parameters
interval: the time interval of hello timer on the interface, the range is 1-65535, the default is 10, and the unit is seconds.

Description
The ip ospf hello-interval command is used to configure the hello timer interval for an interface.
The no ip ospf hello-interval command is used to restore the interface hello timer to its default value.

Examples
Configure the ospf neighbor hello timer interval on interface vlan5 to 5s.

```
switch(config-vlan5)# ip ospf hello-interval 5
switch(config-vlan5)
```

ip ospf message-digest-key

Command

```
ip ospf message-digest-key <key-id> md5 <key-string>
no ip ospf message-digest-key <key-id>
```

Mode
Interface configuration mode.

Parameters
key-id: the id number of the ciphertext authentication, in the range of 1 to 255.
key-string: the string for ciphertext authentication.

Description
The ip ospf message-digest-key command is used to configure the string for ciphertext authentication on the interface.
The no ip ospf message-digest-key command is used to remove the string for ciphertext authentication on the interface.

Examples
Configure the ciphertext authentication word id for ospf on interface vlan5 to be 10 and the string "123pass".

```
switch(config-vlan5)#ip ospf message-digest-key 10 md5 123pass
switch(config-vlan5)#
```

ip ospf mtu

Command

```
ip ospf mtu <mtu>
no ip ospf mtu
```

Mode

Interface configuration mode.

Parameters

mtu: The maximum transmission unit for the port, in the range 576-65535.

Description

The ip ospf mtu command is used to configure the maximum transmission unit of an interface.
The no ip ospf mtu command is used to restore mtu to its default value.

Examples

Configure the maximum transmission unit on interface vlan5 to be 1000.

```
switch(config-vlan5)# ip ospf mtu 1000
switch(config-vlan5)#
```

ip ospf mtu-ignore

Command

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

Mode

Interface configuration mode.

Parameters

None.

Description

The ip ospf mtu-ignore command is used to configure the mtu ignore feature when a DD message is received on the interface, and the mtu bit is not checked when a message is accepted.
The no ip ospf mtu-ignore command is used to restore mtu checking for an interface.

Examples

Configure no mtu checks on interface vlan5.

```
switch(config-vlan5)# ip ospf mtu-ignore
switch(config-vlan5)#
```

ip ospf network

Command

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint [non-broadcast] | point-to-point}
no ip ospf network
```

Mode

Interface configuration mode.

Parameters

broadcast:Broadcast network type.
non-broadcast: Non-broadcast network type.
point-to-multipoint: point-to-multipoint network type.
point-to-point: point-to-point network type.

Description

The ip ospf network command is used to specify the network type where the interface is located. ospf runs the corresponding ospf processing mechanism according to the different network types.
The no ip ospf network command is used to restore the interface to the default network type.

Examples

Configure the network type of interface vlan5 as point-to-point.

```
switch(config-vlan5)# ip ospf network point-to-point
switch(config-vlan5)#
```

ip ospf priority

Command

```
ip ospf priority <priority>
no ip ospf priority
```

Mode

Interface configuration mode.

Parameters

priority: the priority of the interface, the range of 0 to 255, the default value is 1.

Description

The ip ospf priority command is used to specify the interface priority.
The no ip ospf priority command is used to restore the default priority of an interface.

Examples

Configure the priority of interface vlan5 to 10.

```
switch(config-vlan5)# ip ospf priority 10
switch(config-vlan5)#
```

ip ospf retransmit-interval

Command

```
ip ospf retransmit-interval <interval>
no ip ospf retransmit-interval
```

Mode

Interface configuration mode.

Parameters

interval: the time of the retransmit timer on the interface, the range is 1 to 65535, the default is 5, and the unit is seconds.

Description

The ip ospf retransmit-interval command is used to configure the retransmit timer value for an interface.
The no ip ospf retransmit-interval command is used to restore the interface retransmit timer to the default value.

Examples

Configure the retransmi cycle time for ospf on interface vlan5 to 15s.

```
switch(config-vlan5)# ip ospf retransmit-interval 15
switch(config-vlan5)
```

ip ospf transmit- delay

Command

```
ip ospf transmit-delay <interval>
no ip ospf transmit-delay
```

Mode

Interface configuration mode.

Parameters

interval: The transmission delay time on the interface, ranging from 1 to 65535, the default is 40, and the unit is seconds.

Description
The ip ospf transmit-delay command is used to configure the transmission delay value of an interface.
The no ip ospf transmit-delay command is used to restore the interface transmission delay to the default value.

Examples
Configure the transmission delay time for ospf on interface vlan5 to 25s.
```
switch(config-vlan5)# ip ospf transmit-interval 25
switch(config-vlan5)
```

max-concurrent-dd

Command
```
max-concurrent-dd <number>
no max-concurrent-dd
```

Mode
ospf configuration mode.

Parameters
number: the number of DD messages, the range is from 1 to 65535, the default is 5.

Description
The max-concurrent-dd command is used to control the maximum number of DD pending lists. If there is an error during the DD exchange, the neighbor will be put into this pending list.
The no max-concurrent-dd command is used to restore to the default value.

Examples
Configure the maximum number of DD message hangs for ospf 11 to 100.
```
switch(config-router)# max-concurrent-dd 100
switch(config-router)#
```

neighbor

Command
```
neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority <priority>]
no neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority <priority>]
```

Mode
ospf configuration mode.

Parameters
router-id: neighbor router-id, 32-bit dotted decimal.
cost: The cost of the link, takes the value range 1 to 65535.
interval: the time to consider the neighbor dead, the value range is 1 to 65535, in seconds.
priority: the priority of the DR election, the value range 0 to 255.

Description
The neighbor command is used to specify a neighbor on the NBMA network and configure related parameters.
The no neighbor command is used to cancel a neighbor specified on the NBMA network.

Examples
Configure neighbor 1.1.1.2 on the NBMA network with a negotiation priority of 10.
```
switch(config-router)# neighbor 1.1.1.2 priority 10
switch(config-router)#
```

network

Command
```
network <network> area <area-id>
no network <network> area <area-id>
```

Mode
ospf configuration mode.

Parameters
network: the network to enable ospf, network/mask or network + reverse mask form.
area-id: area id, in 32-dot decimal or numeric form.

Description
The network command is used to enable a network and specify the area to join.
The no network command is used to cancel the enablement of a network.

Examples
Configure to enable network 172.20.1.0/24 into area 0 of ospf 11.

```
switch(config-router)# network 172.20.1.0/24 area 0
switch(config-router)#
```

passive-interface

Command

```
passive-interface <if-name><if-address>
no passive-interface <if-name><if-address>
```

Mode
ospf configuration mode.

Parameters
if-name: Interface name.
if-address: interface address, 32-bit dotted decimal form.

Description
The passive-interface command is used to configure the interface as a passive interface, after which the interface can receive ospf messages but cannot send ospf messages.
The no passive-interface command is used to restore the interface to the transceiver state.

Examples
Configure interface vlan55 as a passive interface.

```
switch(config-router)#passive-interface vlan55 172.20.10.1
switch(config-router)#
```

redistribute

Command

```
redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]
no redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]
```

Mode
ospf configuration mode.

Parameters
protocol:The type of routing protocol to be introduced into ospf.
metric: Specifies the metric value of the introduced route.
type: the type of route introduced, takes the value of 1 or 2, the default is 2.
route-map: the name of the route-map to be referenced when introducing routes.
tag: introduce the routing tag.

Description
redistribute is used to introduce routes from other protocols into ospf.
no redistribute is used to cancel the introduction of routes to other protocols. By default, no routes are introduced.

Examples

```
#Introduce directly connected routes into the ospf routing table, and specify the metric value of the
introduced routes as 9 by the route-map rule "list123" rule.
```

```
switch(config-router)#redistribute connected metric 9 route-map list123
switch(config-router)#
```

router ospf

Command

```
router ospf [<process-id>]
no router ospf [<process-id>]
```

Mode

Global configuration mode.

Parameters

process-id: ospf process number, the range is from 1 to 65535, the default value is 0.

Description

The router ospf command is used to create an ospf process and enter the process in configuration mode.
The no router ospf command is used to delete an ospf process and the configuration under that process.

Examples

```
#Create ospf process 11.
switch(config)#router ospf 11
switch(config-router)#
```

router-id

Command

```
router-id <router-id>
no router-id [<router-id>]
```

Mode

ospf configuration mode.

Parameters

router-id: router id, in dotted decimal format.

Description

The router-id command is used to configure the router-id of an ospf process. The system needs a unique identity in the AS when negotiating ospf with its neighbors. When not configured, the largest interface ip address is used as the router-id.
The no router-id command is used to remove the configured router-id, which is selected using the default method.

Examples

Configure the ospf process to use router-id 1.1.1.10.

```
switch(config-router)# router-id 1.1.1.10
switch(config-router)#
```

summary-address

Command

```
summary-address <ip-prefix> [not-advertise] [tag <tag>]
no summary-address <ip-prefix> [not-advertise] [tag <tag>]
```

Mode

ospf configuration mode.

Parameters

ip-prefix: the range of routes to be aggregated, in network/mask form.
not-advertise: No detailed route is notified after aggregation.
tag: Specifies the tag value of the aggregated route.

Description
The summary-address command is used to suppress or aggregate externally introduced routes. Routes introduced from other protocols can be aggregated to a certain range using this command. After aggregation, routes within the coverage of this prefix are suppressed, and only one of the aggregated routes is broadcast. prefix indicates only a route range, and the introduced external routes need not be contiguous within this range
The no summary-address command is used to delete the configured route aggregation.

Examples
Configure the ospf process to use route aggregation.
```
switch(config-router)#summary-address 1.1.0.0/20
switch(config-router)#
```

timers spf

Command
```
timers spf <delay><hold>
no timers spf <delay><hold>
```

Mode
ospf configuration mode.

Parameters
delay: delay time, default is 5s.
hold: Inhibit time, default is 10s.

Description
The timers spf command is used to configure the delay time and suppression time of the spf calculation timer. Each time the spf calculation is started, the suppression time from the last spf calculation to the present is calculated. If the configured suppression time has been exceeded, the timer is started directly using the configured delay time; if the configured suppression time has not been exceeded, the time that still needs to be delayed is calculated using the configured suppression time, and if this delay time is too small and smaller than the configured delay time, the configured delay time is used, otherwise the timer is started using the calculated delay time.
The no timers spf command is used to restore the spf calculation timers to their default values.

Examples
Configure ospf to perform spf calculations with a delay time of 10s and a suppression time of 15s.
```
switch(config-router)#timers spf 10 15
switch(config-router)#
```

View command

show ip ospf

Command
```
show ip ospf [<process-id>]
```

Mode
Privilege mode / Normal mode.

Parameters
process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description
The show ip ospf command is used to display information about the specified ospf process. When no process number is specified, information about all currently existing processes is displayed.

Examples
Display information about ospf process 10.
```
switch#show ip ospf 10
```

```
Routing Process "ospf 10" with ID 192.168.0.1
Process uptime is 1 day 7 hours 52 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 1. Checksum 0x007741
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 69
Number of LSA received 192
Number of areas attached to this router: 2
Area 0 (BACKBONE)
Number of interfaces in this area is 17(17)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 31:09:58.285 ago
SPF algorithm executed 10 times
Number of LSA 5. Checksum 0x023ca6
Area 1
Number of interfaces in this area is 2(2)
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 31:52:10.025 ago
SPF algorithm executed 4 times
Number of LSA 20. checksum 0x09f53d
switch#
```

show ip ospf database

Command

```
show ip ospf [<process-id>] database [adv-router | asbr-summary | external | max-age | network |
nssa-external | opaque-area | opaque-as | opaque -link | router | self-originate | summary]
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.
adv-router: Advertise routing link status information.
asbr-summary: summary link status information of asbr.
external: External routing link status information.
max-age: link status information in the age list.
network: Network type link status information.
nssa-external: Link status information introduced by the NSSA area.
router: router link status information
self-originate: Self-generated link state information.
summary: Network aggregation link status information.

Description

The show ip ospf [<process-id>] database command is used to display the link state database information for the specified ospf process.

Examples

Display information about networks type in the link state database for ospf process 10.

```
switch#show ip ospf 10 database network
OSPF Router with ID (192.168.0.1) (Process ID 10)
Net Link States (Area 0.0.0.0)
LS age: 531
Options: 0x22 (*|-|DC|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 172.20.5.3 (address of Designated Router)
Advertising Router: 192.168.130.2
LS Seq Number: 8000003e
Checksum: 0xe30a
Length: 32
Network Mask: /24
Attached Router: 192.168.130.2
Attached Router: 192.168.0.1
switch#
```

show ip ospf interface

Command

```
show ip ospf interface [<if-name>]
```

Mode

Privilege mode / Normal mode.

Parameters

if-name: the name of the interface that needs to display information about the ospf interface.

Description

The show ip ospf interface command is used to display ospf-related information of an interface.

Examples

Display information about interfaces with the ospf protocol activated.

```
switch# show ip ospf interface
vlan5 is up, line protocol is up
Internet Address 172.20.22.225/27, Area 0.0.0.1, MTU 1500
Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.20.22.225, Interface Address 172.20.22.225
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 3774326953
Hello received 0 sent 5, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
vlan6 is down, line protocol is down
OSPF is enabled, but not running on this interface
vlan51 is up, line protocol is up
Internet Address 172.20.6.2/24, Area 0.0.0.0, MTU 1500
Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.20.22.225, Interface Address 172.20.6.2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 3774326953
```

```
Hello received 0 sent 5, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
switch#
```

show ip ospf neighbor

Command

```
show ip ospf [<process-id>] neighbor [<neighbor-id>] | [all | detail | interface <if-address>]
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.
neighbor-id: neighbor router ID.
all: Show all neighbors, including those in down status.
detail: Displays detailed information about the neighbor.
interface if-address: View the neighbor information on the specified interface.

Description

The show ip ospf [<process-id>] neighbor command is used to display the neighbor information of ospf.

Examples

Display neighbor information on interface address 172.20.5.2 for ospf process 10.

```
switch#show ip ospf nei inter 172.20.5.2
OSPF process 10
Neighbor ID Pri State Dead Time Address Interface
192.168.130.2 1 Full/DR 00:00:34 172.20.5.3 vlan10
switch#
```

show ip ospf route

Command

```
show ip ospf [<process-id>] route [count]
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.
count: show the number of ospf routes.

Description

The show ip ospf [process-id] route command is used to display the ospf routing table.

Examples

Display the number of ospf route entries for ospf process 10.

```
switch#show ip ospf 10 route coun
total routes: 21
switch#
```

show ip ospf virtual-links

Command

```
show ip ospf [<process-id>] virtual-links
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description

The show ip ospf [<process-id>] virtual-links command is used to view information about virtual connections.

Examples

Display ospf virtual link information for ospf process 10.

```
switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.10 is down
Transit area 0.0.0.1 via interface *
Local address *
Remote address *
Transmit Delay is 1 sec, State Down,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in inactive
Adjacency state Down
switch#
```

show running ospf

Command

```
show running ospf
```

Mode

Privilege mode / Normal mode.

Parameters

None.

Description

The show running ospf command is used to view the ospf configuration information on the current system.

Examples

Display the current ospf configuration information on the system.

```
switch#show running-config ospf
!
router ospf
!
router ospf 1
!
router ospf 10
network 172.20.5.0/24 area 0
network 172.20.6.0/24 area 0
network 172.20.7.0/24 area 0
network 172.20.11.0/24 area 0
network 172.20.22.192/27 area 1
network 172.20.22.224/27 area 1
area 1 virtual-link 1.1.1.10
!
router ospf 11
area 1 authentication message-digest
area 1 nssa default-information-originate no-summary
!
switch#
```

Debugging commands

debug ospf

Command

```
debug ospf
no debug ospf
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ospf command is used to turn on the ospf-related debug switch to enable users to see the ospf-related negotiation process and message sending and receiving.
The no debug ospf command is used to turn off the ospf debug switch

Examples

```
#Turn on the debug switch to display ospf debug information
switch#debug ospf
switch#
```

debug ospf all

Command

```
debug ospf all
no debug ospf all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ospf all command is used to turn on all debug switches related to ospf, so that users can see the negotiation process and message sending and receiving related to ospf.
The no debug ospf all command is used to turn off all debug switches related to ospf.

Examples

```
#Turn on the debug switch to show all debug information of ospf
switch#debug ospf all
switch#
```

debug ospf events

Command

```
debug ospf events
no debug ospf events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ospf events command is used to turn on the ospf events debug switch to enable users to see ospf-related event information.

The no debug ospf events command is used to turn off the ospf events debug switch.

Examples

```
#Turn on debug switch to display ospf event information
switch#debug ospf events
switch#
```

debug ospf ifsm

Command

```
debug ospf ifsm
no debug ospf ifsm
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ospf ifsm command is used to turn on the ospf interface status debug switch to enable users to see the ospf interface status machine change information.
The no debug ospf ifsm command is used to turn off the interface state machine debug switch.

Examples

```
#Turn on the debug switch to show the ospf interface status change information
switch#debug ospf ifsm
switch#
```

debug ospf lsa

Command

```
debug ospf lsa
no debug ospf lsa
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ospf lsa command is used to turn on the ospf lsa-related debug switch to enable users to see the lsa sending and receiving information.
The no debug ospf lsa command is used to turn off the ospf lsa debug switch.

Examples

Turn on the debug switch and show the ospf lsa information

```
switch#debug ospf lsa
switch#
```

debug ospf nfsm

Command

```
debug ospf nfsm
no debug ospf nfsm
```

Mode

Privilege mode.

Parameters

None.

Description
The debug ospf nfsm command is used to turn on the ospf neighbor status debug switch to enable users to see the ospf neighbor status changes.
The no debug ospf nfsm command is used to turn off the ospf neighbor status debug switch.

Examples
```
#Turn on the debug switch to display ospf neighbor status change information
switch#debug ospf nfsm
switch#
```

debug ospf packet

Command
```
debug ospf packet [recv | send] [detail]
no debug ospf packet [recv | send] [detail]
```

Mode
Privilege mode.

Parameters
recv: receive message information.
send: Send message information.
detail: Detailed information.

Description
The debug ospf packet command is used to turn on the ospf packet debug switch to enable users to see the sending and receiving of ospf packets.
The no debug ospf packet command is used to turn off the ospf packet debug switch.

Examples
```
#Turn on the debug switch to show the details of the hello message
switch#debug ospf packet hello detail
switch#
```

debug ospf route

Command
```
debug ospf route
no debug ospf route
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ospf route command is used to turn on the ospf route debug switch to enable users to see the ospf route debug information.
The no debug ospf route command is used to turn off the ospf route debug switch.

Examples
```
#Turn on the debug switch to display ospf routing debug information
switch#debug ospf route
switch#
```

CHAPTER 30

OSPFv3 commands

Configuration commands

router ipv6 ospf

Command

```
router ipv6 ospf [<process-id>]
no router ipv6 ospf [<process-id>]
```

Mode

Global configuration mode.

Parameters

process-id: ospf process number, the range is from 1 to 65535, the default value is 0.

Description

The router ipv6 ospf command is used to create the ospfv3 process and enter the process in configuration mode. The no router ipv6 ospf command is used to delete an ospfv3 process and the configuration under that process.

Examples

```
#Create ospfv3 process 11.
switch(config)#router ipv6 ospf 11
switch(config-router)#
```

ipv6 routerospf

Command

```
ipv6 router ospf area <area-id> [tag<process-tag>|instance-id< instance-id>]
no ipv6 router ospf area <area-id> [tag <process-tag> |instance-id< instance-id> ]
```

Mode

Interface configuration mode

Parameters

area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
process-tag: Process TAG.
instance-id: The instance ID of the interface, in the range 0 to 255.

Description

The ipv6 router rip command is used to start the RIPng protocol for an interface.
The no ripv6 router rip command is used to turn off the RIPng protocol for the interface.

Examples

Start the RIPng protocol for interface vlan1.

```
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#switch(config-router)#
```

area default-cost

Command

```
area <area-id> default-cost <cost>
no area <area-id> default-cost
```

Mode
OSPFv3 configuration mode.

Parameters
area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
cost: Routing splurge value, takes the value range 0 to 16777215.

Description
The area <area-id> default-cost command is used to configure the default cost of summary routes sent from the ABR to the stub area and the nssa area.
The no area <area-id> default-cost command is used to cancel the default spend configuration for an area and restore it to the default value.

Examples
```
#Configure the default cost for area 1 to 224.
switch(config-router)#area 1 default-cost 224
switch(config-router)#
```

area range

Command
```
area <area-id> range <ipv6-prefix> [advertise | not-advertise]
no area <area-id> range <ipv6-prefix> [advertise | not-advertise]
```

Mode
Ospfv3 configuration mode.

Parameters
area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
ipv6-prefix: The aggregated routing range, network/mask format.
advertise: Advertise the aggregated route after aggregation.
not-advertise: routes that are not advertised for aggregation.

Description
The area <area-id> range command is used to configure route aggregation or additional parameters within an area.
The no area <area-id> range command is used to cancel route aggregation for an area or remove additional parameters.

Examples
Configure area 1 of ospf process 11 for route aggregation and advertise the aggregated route.
```
switch(config-router)#area 1 range 3ffe:506::/64 advertise
switch(config-router)#
```

area stub

Command
```
area <area-id> stub [no-summary]
no area <area-id> stub [no-summary]
```

Mode
Ospfv3 configuration mode.

Parameters
area-id: ospf area id, can be expressed in decimal, the value range is 0~4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
no-summary: Configure the ABR not to advertise summary routes to the stub area. By default, notification is allowed.

Description
The area <area-id> stub command is used to specify the area as the stub area.
The no area <area-id> stub command is used to unspecify an area as a stub area.

Examples
Configure area 1 of ospf process 11 as a stub area, without learning summary routes.
```
switch(config-router)#area 1 stub no-summary
switch(config-router)#
```

area virtual-link

Command
```
area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval
<hello-interval>] [ retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]
no area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval
<hello-interval>] [ retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]
```

Mode
Ospfv3 configuration mode.

Parameters
area-id: the id of the ospf area, can be expressed in decimal, the value range is 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.
neighbor-id: Router-id of the router on the opposite end of the virtual connection.
dead-interval: Configure the death time for router failure on a dummy connection. The default is 4 times the hello message period (40s).
hello-interval: Configure the time interval for hello messages to be sent on a virtual connection. The default is 10s.
retran-interval: Configures the message retransmission interval on a virtual connection. The default is 5s.
delay-interval: Configure the delay time for message transmission on a virtual connection. The default is 40s.

Description
The area <area-id> virtual-link command is used to configure a virtual connection and related parameters.
The no area <area-id> virtual-link command is used to remove the virtual link or restore the parameters on the virtual link to the default configuration.

Examples
Configure the virtual connection with neighbor 1.1.1.1 in area 1 of ospf process 11 with a hello interval of 5s.
```
switch(config-router)#area 1 virtual-link 1.1.1.1 hello-interval 5
switch(config-router)#
```

auto-cost reference-bandwidth

Command
```
auto-cost reference-bandwidth <bandwidth>
no auto-cost reference-bandwidth
```

Mode
Ospfv3 configuration mode.

Parameters
bandwidth: the reference bandwidth in Mbits/s, the range is 1 to 4294967, the default is 10000Mbits/s.

Description
The auto-cost reference-bandwidth command is used to configure the reference bandwidth value, and the ospfv3 protocol calculates the spend of the route based on the configured value.
The no auto-cost reference-bandwidth command is used to remove the configuration of the reference bandwidth value and restore it to the default value.

Examples
Configure ospf process 11 with a reference bandwidth of 1000Mbits/s.
```
switch(config-router)#auto-cost reference-bandwidth 1000
```

```
switch(config-router)#
```

default-metric

Command

```
default-metric <metric>
no default-metric [<metric>]
```

Mode

Ospfv3 configuration mode.

Parameters

metric: the default spend of the introduced route, the value range is 0 to 16777214, the default is 1.

Description

The default-metric command is used to configure the default metric value of the route introduced by ospfv3.
The no default-metric command is used to restore the metric value of the introduced route to the default value.

Examples

Configure ospf process 11 to introduce routes with a default metric of 12.

```
switch(config-router)#default-metric 12
switch(config-router)#
```

distance

Command

```
distance {<distance> | ospfv3 external <distance> | ospfv3 inter-area <distance> | ospfv3 intra-area
<distance>}
no distance {<distance> | ospfv3 external <distance> | ospfv3 inter-area <distance> | ospfv3
intra-area <distance>}
```

Mode

Ospfv3 configuration mode.

Parameters

distance: the administrative distance of the route, the value range is 1 to 255, the default is 110.
external: The external route obtained through route introduction.
inter-area: Inter-area routing.
intra-area: Intra-area routing.

Description

The distance command is used to configure the administrative distance of ospfv3 routes.
The no distance command is used to restore the administrative distance of ospfv3 routes to the default value.

Examples

Configure ospf routes with an administrative distance of 120.

```
switch(config-router)#distance 120
switch(config-router)#
```

distribute-list

Command

```
distribute-list <acl-list><in | out <protocol>>
no distribute-list <acl-list><in | out <protocol>>
```

Mode

Ospfv3 configuration mode.

Parameters

acl-list: the name of the access control list.
in: Filter while inward.
out: Filter when announcing routes to the outside.

protocol: Specifies the target protocol for the filtering implementation.

Description
The distribute-list command is used to configure the filtering of introduced routes when ospfv3 advertises routes. The no distribute-list command is used to cancel route filtering.

Examples
Configure the ospfv3 announcement route to filter the introduced rip routes using an acl named list123.

```
switch(config-router)# distribute-list list123 out rip
switch(config-router)#
```

max-concurrent-dd

Command

```
max-concurrent-dd <number>
no max-concurrent-dd
```

Mode
Ospfv3 configuration mode.

Parameters
number: the number of DD messages, the range is from 1 to 65535, the default is 5.

Description
The max-concurrent-dd command is used to control the maximum number of DD pending lists. If there is an error during the DD exchange, the neighbor will be put into this pending list.
The no max-concurrent-dd command is used to restore to the default value.

Examples
Configure the maximum number of DD message hangs for ospf 11 to 100.

```
switch(config-router)# max-concurrent-dd 100
switch(config-router)#
```

passive-interface

Command

```
passive-interface <if-name>
no passive-interface <if-name>
```

Mode
Ospfv3 configuration mode.

Parameters
if-name: Interface name.

Description
The passive-interface command is used to configure the interface as a passive interface. After configuration, the interface can receive ospfv3 messages, but cannot send ospfv3 messages.
The no passive-interface command is used to restore the interface to the transceiver state.

Examples
Configure interface vlan55 as a passive interface.

```
switch(config-router)#passive-interface vlan55
switch(config-router)#
```

redistribute

Command

```
redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]
no redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]
```

Mode
Ospfv3 configuration mode.

Parameters
protocol:The type of routing protocol to be introduced into ospfv3.
metric: Specifies the metric value of the introduced route.
type: the type of route introduced, takes the value of 1 or 2, the default is 2.
route-map: the name of the route-map to be referenced when introducing routes.
tag: introduce the routing tag.

Description
redistribute is used to introduce routes from other protocols into ospfv3.
no redistribute is used to cancel the introduction of routes to other protocols. By default, no routes are introduced.

Examples
```
#Introduce directly connected routes into the ospfv3 routing table, and specify the metric value of
the introduced routes as 9 by the route-map rule "list123".
switch(config-router)#redistribute connected metric 9 route-map list123
switch(config-router)#
```

router-id

Command
```
router-id <router-id>
no router-id [<router-id>]
```

Mode
Ospfv3 configuration mode.

Parameters
router-id: router id, in dotted decimal format.

Description
The router-id command is used to configure the router-id of an ospfv3 process. The system needs a unique identity in the AS when negotiating ospfv3 with its neighbors. The largest interface ip address is used as the router-id when not configured.
The no router-id command is used to remove the configured router-id, which is selected using the default method.

Examples
Configure the ospf process to use router-id 1.1.1.10.
```
switch(config-router)# router-id 1.1.1.10
switch(config-router)#
```

timers spf

Command
```
timers spf <delay><hold>
no timers spf <delay><hold>
```

Mode
Ospfv3 configuration mode.

Parameters
delay: delay time, default is 5s.
hold: Inhibit time, default is 10s.

Description

The timers spf command is used to configure the delay time and suppression time of the spf calculation timer. Each time the spf calculation is started, the suppression time from the last spf calculation to the present is calculated. If the configured suppression time has been exceeded, the timer is started directly using the configured delay time; if the configured suppression time has not been exceeded, the time that still needs to be delayed is calculated using the configured suppression time, and if this delay time is too small and smaller than the configured delay time, the configured delay time is used, otherwise the timer is started using the calculated delay time.
The no timers spf command is used to restore the spf calculation timers to their default values.

Examples
Configure ospfv3 to perform spf calculations with a delay time of 10s and a suppression time of 15s.
```
switch(config-router)#timers spf 10 15
switch(config-router)#
```

ipv6 ospf cost

Command
```
Ipv6 ospf cost <cost> [instance-id< instance-id>]
no ip ospf cost [instance-id< instance-id>]
```

Mode
Interface configuration mode.

Parameters
cost: The link spend of the interface, the value range is 1 to 65535.
instance-id: The instance ID of the interface, in the range 0 to 255.

Description
The Ipv6 ospf cost command is used to configure the link spend of the interface, which is valid for outgoing interface routes.
The no ipv6 ospf cost command is used to restore the link spend of an interface to the default value.

Examples
Configure the link spend for interface vlan5 to 23.
```
switch(config-vlan5)#ipv6 ospf cost 23
switch(config-vlan5)
```

ipv6 ospf dead-interval

Command
```
Ipv6 ospf dead-interval <interval>
no ipv6 ospf dead-interval
```

Mode
Interface configuration mode.

Parameters
interval: the time of the dead timer on the interface, the value range is 1 to 65535, the default is 40 on the broadcast network, and the unit is seconds.

Description
The Ipv6 ospf dead-interval command is used to configure the dead timer value of an interface.
The no ipv6 ospf dead-interval command is used to restore the interface dead timer to the default value.

Examples
Configure the ospf neighbor dead time on interface vlan5 to 20s.
```
switch(config-vlan5)# ip ospf dead-interval 20
switch(config-vlan5)
```

ipv6 ospf hello-interval

Command

```
Ipv6 ospf hello-interval <interval>
no ipv6 ospf hello-interval
```

Mode

Interface configuration mode.

Parameters

interval: the time interval of hello timer on the interface, the range is 1-65535, the default is 10, and the unit is seconds.

Description

The Ipv6 ospf hello-interval command is used to configure the hello timer interval of an interface.
The no ipv6 ospf hello-interval command is used to restore the interface hello timer to the default value.

Examples

Configure the ospfv3 neighbor hello timer interval on interface vlan5 to 5s.

```
switch(config-vlan5)# ipv6 ospf hello-interval 5
switch(config-vlan5)
```

ipv6 ospf mtu-ignore

Command

```
Ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore
```

Mode

Interface configuration mode.

Parameters

None.

Description

The Ipv6 ospf mtu-ignore command is used to configure the mtu ignore function when a DD message is received on the interface, and the mtu bit is not checked when a message is accepted.
The no ipv6 ospf mtu-ignore command is used to restore mtu checking on an interface.

Examples

Configure no mtu checks on interface vlan5.

```
switch(config-vlan5)# ipv6 ospf mtu-ignore
switch(config-vlan5)#
```

ipv6 ospf network

Command

```
Ipv6 ospf network {broadcast | non-broadcast | point-to-multipoint [non-broadcast] | point-to-point}
no ipv6 ospf network
```

Mode

Interface configuration mode.

Parameters

broadcast:Broadcast network type.
non-broadcast: Non-broadcast network type.
point-to-multipoint: point-to-multipoint network type.
point-to-point: point-to-point network type.

Description

The Ipv6 ospf network command is used to specify the network type where the interface is located. ospfv3 runs the corresponding ospfv3 processing mechanism according to the different network types.

The no ipv6 ospf network command is used to restore the interface to the default network type.

Examples

Configure the network type of interface vlan5 as point-to-point.

```
switch(config-vlan5)# ipv6 ospf network point-to-point
switch(config-vlan5)#
```

ipv6 ospf priority

Command

```
Ipv6 ospf priority <priority> [instance-id< instance-id>]
no ipv6 ospf priority [instance-id< instance-id>]
```

Mode

Interface configuration mode.

Parameters

priority: the priority of the interface, the range of 0 to 255, the default value is 1.
instance-id: The instance ID of the interface, in the range of 0 to 255.

Description

The Ipv6 ospf priority command is used to specify the interface priority.
The no ipv6 ospf priority command is used to restore the default priority of an interface.

Examples

Configure the priority of interface vlan5 to 10.

```
switch(config-vlan5)# ipv6 ospf priority 10
switch(config-vlan5)#
```

ipv6 ospf retransmit-interval

Command

```
Ipv6 ospf retransmit-interval <interval> [instance-id< instance-id>]
no ipv6 ospf retransmit-interval [instance-id< instance-id>]
```

Mode

Interface configuration mode.

Parameters

interval: the time of the retransmit timer on the interface, the range is 1 to 65535, the default is 5, and the unit is seconds.
instance-id: The instance ID of the interface, in the range of 0 to 255.

Description

The Ipv6 ospf retransmit-interval command is used to configure the retransmit timer value of an interface.
The no ipv6 ospf retransmit-interval command is used to restore the interface retransmit timer to the default value.

Examples

Configure the retransmi cycle time for ospfv3 on interface vlan5 to 15s.

```
switch(config-vlan5)# ipv6 ospf retransmit-interval 15
switch(config-vlan5)
```

ipv6 ospf transmit-delay

Command

```
Ipv6 ospf transmit-delay <interval> [instance-id< instance-id>]
no ipv6 ospf transmit-delay [instance-id< instance-id>]
```

Mode

Interface configuration mode.

Parameters
interval: The transmission delay time on the interface, ranging from 1 to 65535, the default is 40, and the unit is seconds.
instance-id: The instance ID of the interface, in the range of 0 to 255.

Description
The Ipv6 ospf transmit-delay command is used to configure the transmission delay value of an interface.
The no ipv6 ospf transmit-delay command is used to restore the interface transmission delay to the default value.

Examples
Configure the transmission delay time for ospfv3 on interface vlan5 to 25s.

```
switch(config-vlan5)# ipv6 ospf transmit-interval 25
switch(config-vlan5)
```

View command

show ipv6 ospf

Command

```
show ipv6 ospf [<process-id>]
```

Mode
Privilege mode / Normal mode.

Parameters
process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description
The show ipv6 ospf command is used to display information about the specified ospfv3 process. When the process number is not specified, information about all currently existing processes is displayed.

Examples
Display information about ospfv3.

```
Switch#show ipv6 ospf
Routing Process "OSPFv3 (*null*)" with ID 1.1.1.1
Process uptime is 4 minutes
SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 5
Number of LSA received 5
Number of areas in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1(1)
SPF algorithm executed 6 times
Number of LSA 4. Checksum Sum 0x2CDA4
Number of Unknown LSA 0
```

show ipv6 ospf database

Command

```
show ipv6 ospf [<process-id>] database [adv-router | external | max-age | network | router |
self-originate]
```

Mode
Privilege mode / Normal mode.

Parameters
process-id: process number, specifying the process to be viewed, in the range 0 to 65535.
adv-router: Advertise routing link status information.
external: External routing link status information.
max-age: link status information in the age list.
network: Network type link status information.
router: router link status information
self-originate: Self-generated link state information.

Description
The show ip ospf [<process-id>] database command is used to display the link state database information for the specified ospf process.

Examples
Display link status database information for ospfv3 process 10.

```
Switch#show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process *null*)
Link-LSA (Interface vlan1)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.6 1.1.1.1 193 0x8000000b 0xa641 1
0.0.0.6 5.5.5.5 1188 0x8000000a 0xcd1c 1
Router-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Link
0.0.0.0 1.1.1.1 1172 0x8000000c 0x45ba 1
0.0.0.0 5.5.5.5 1168 0x8000000c 0xcc23 1
Network-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum
0.0.0.6 1.1.1.1 1172 0x8000000a 0xe01d
Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.2 1.1.1.1 1172 0x8000000a 0x9dc5 1 Network-LSA
```

show ipv6 ospf interface

Command

```
show ipv6 ospf interface [<if-name>]
```

Mode
Privilege mode / Normal mode.

Parameters
if-name: the name of the interface that needs to display information about the ospf interface.

Description
The show ipv6 ospf interface command is used to display ospfv3-related information of an interface.

Examples
Display information about interfaces that have the ospfv3 protocol enabled.

```
Switch#show ipv6 ospf interface
vlan1 is up, line protocol is up
Interface ID 6
IPv6 Prefixes
fe80::82:44ff:fe13:4803/64 (Link-Local Address)
3ffe:506::1/64
OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
```

```
Designated Router (ID) 1.1.1.1
Interface Address fe80::82:44ff:fe13:4803
Backup Designated Router (ID) 5.5.5.5
Interface Address fe80::2a7:c1ff:fed1:5581
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Switch#
```

show ipv6 ospf neighbor

Command

```
show ip ospf [<process-id>] neighbor [<neighbor-id>] | [detail | interface <if-address>]
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.
neighbor-id: neighbor router ID.
detail: Displays detailed information about the neighbor.
interface if-address: View the neighbor information on the specified interface.

Description

The show ipv6 ospf [<process-id>] neighbor command is used to display the neighbor information of ospf.

Examples

Display neighbor information for ospfv3.

```
Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID Pri State Dead Time Interface Instance ID
5.5.5.5 1 Full/Backup 00:00:38 vlan1 0
Switch#
```

show ipv6 ospf route

Command

```
show ipv6 ospf [<process-id> route
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description

The show ipv6 ospf [process-id] route command is used to display the ospfv3 routing table.

Examples

Display ospfv3 routing information.

```
Switch#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2
Destination Metric
Next-hop
C 3ffe:506::/64 1
directly connected, vlan1, Area 0.0.0.0
Switch#
```

show ipv6 ospftopology

Command

```
show ipv6 ospf [<process-id>topology
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description

The show ipv6 ospf [process-id] topology command is used to display ospfv3 topology information.

Examples

Display ospfv3 topology information.

```
Switch#show ipv6 ospf topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID Bits Metric Next-Hop Interface
1.1.1.1 -
5.5.5.5 1 5.5.5.5 vlan1
```

show ipv6 ospf virtual-links

Command

```
show ipv6 ospf [<process-id>] virtual-links
```

Mode

Privilege mode / Normal mode.

Parameters

process-id: process number, specifying the process to be viewed, in the range 0 to 65535.

Description

The show ipv6 ospf [<process-id>] virtual-links command is used to view information about virtual connections.

Examples

Display ospfv3 virtual link information.

```
Switch#show ipv6 ospf virtual-links
```

Debugging commands

debug ipv6 ospf

Command

```
debug ipv6 ospf
no debug ipv6 ospf
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ipv6 ospf command is used to turn on the ospfv3-related debug switch to enable users to see the ospfv3-related negotiation process and message sending and receiving.
The no debug ipv6 ospf command is used to turn off the ospfv3 debug switch

Examples

```
#Turn on the debug switch to display ospfv3 debug information
switch#debug ipv6 ospf
switch#
```

debug ipv6 ospf all

Command

```
debug ipv6 ospf all
no debug ipv6 ospf all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ipv6 ospf all command is used to turn on all debug switches related to ospfv3, enabling users to see the negotiation process and message sending and receiving related to ospfv3.
The no debug ipv6 ospf all command is used to turn off all debug switches related to ospfv3.

Examples

```
#Turn on the debug switch to show all debug information of ospfv3
switch#debug ipv6 ospf all
switch#
```

debug ospf events

Command

```
debug ipv6 ospf events
no debug ipv6 ospf events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug ipv6 ospf events command is used to turn on the ospfv3 event debug switch to enable users to see ospfv3-related event information.
The no debug ipv6 ospf events command is used to turn off the ospfv3 event debug switch.

Examples

Turn on the debug switch to display ospfv3 event information

```
switch#debug ipv6 ospf events
switch#
```

debug ipv6 ospf ifsm

Command

```
debug ipv6 ospf ifsm
no debug ipv6 ospf ifsm
```

Mode

Privilege mode.

Parameters

None.

Description
The debug ipv6 ospf ifsm command is used to turn on the ospfv3 interface state debug switch to enable users to see the ospfv3 interface state machine change information.
The no debug ipv6 ospf ifsm command is used to turn off the interface state machine debug switch.

Examples
```
#Turn on the debug switch to show the ospfv3 interface status change information
switch#debug ipv6 ospf ifsm
switch#
```

debug ipv6 ospf lsa

Command
```
debug ipv6 ospf lsa
no debug ipv6 ospf lsa
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ipv6 ospf lsa command is used to turn on the ospfv3 lsa-related debug switch to enable users to see lsa send and receive information.
The no debug ipv6 ospf lsa command is used to turn off the ospfv3 lsa debug switch.

Examples
Turn on the debug switch and show the ospfv3 lsa information
```
switch#debug ipv6 ospf lsa
switch#
```

debug ipv6 ospf nfsm

Command
```
debug ipv6 ospf nfsm
no debug ipv6 ospf nfsm
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ipv6 ospf nfsm command is used to turn on the ospfv3 neighbor status debug switch to enable users to see the ospfv3 neighbor status changes.
The no debug ipv6 ospf nfsm command is used to turn off the ospfv3 neighbor status debug switch.

Examples
```
#Turn on the debug switch to display ospfv3 neighbor status change information
switch#debug ipv6 ospf nfsm
switch#
```

debug ipv6 ospf packet

Command
```
debug ipv6 ospf packet [recv | send | dd | hello | ls-request | ls-update] [detail]
no debug ipv6 ospf packet [recv | send | dd | hello | ls-request | ls-update] [detail]
```

Mode
Privilege mode.

Parameters
recv: receive message information.
send: Send message information.
detail: Detailed information.

Description
The debug ipv6 ospf packet command is used to turn on the ospfv3 packet debug switch to enable users to see the sending and receiving of ospfv3 packets.
The no debug ipv6 ospf packet command is used to turn off the ospfv3 packet debug switch.

Examples
```
#Turn on the debug switch to show the details of the hello message
switch#debug ipv6 ospf packet hello detail
switch#
```

debug ipv6 ospf route

Command
```
debug ipv6 ospf route
no debug ipv6 ospf route
```

Mode
Privilege mode.

Parameters
None.

Description
The debug ipv6 ospf route command is used to turn on the ospfv3 routing debug switch to enable users to see ospfv3 routing debug information.
The no debug ipv6 ospf route command is used to turn off the ospfv3 routing debug switch.

Examples
Turn on the debug switch to display ospfv3 routing debug information
```
switch#debug ipv6 ospf route
switch#
```

CHAPTER 31

BGP Commands

Configuration commands

router bgp

Command

```
router bgp<as-number>[view <view-name>]
no router bgp <as-number> [view <view-name>]
```

Mode

Global configuration mode.

Parameters

as-number: as number, the value range is 1 to 4294967295.
view-name: view name

Description

The router bgp command starts BGP and enters BGP configuration mode.
The no router bgp command is used to delete a BGP process and the configuration under that process.

Examples

Create BGPAS number 11.

```
switch(config)#router BGP 11
switch(config-router)#
```

address-family

Command

```
address-family<ipv4 | ipv6> [multicast | unicast]
```

Mode

BGP configuration mode.

Parameters

multicast: optional, enter ipv4 multicast address family mode.
unicast: optional, enter ipv4/ipv6 multicast address family mode.

Description

The address-family command is used to enter the address family configuration mode of BGP.

Examples

Enter IPV4 address family configuration mode.

```
Switch(config)#router bgp 1
Switch(config-router)#address-family ipv4
Switch(config-router-af)#
```

aggregate-address

Command

```
aggregate-address<ip-address>/<mask-length>[as-set| summary-only] no
aggregate-address<ip-address>/<mask-length>[as-set| summary-only]
```

Mode

BGP configuration mode/IPv6 address family configuration mode for BGP.

Parameters
ip-address: destination ipv4/ipv6 address prefix.
mask-length: aggregation address mask, expressed in decimal.
as-set:Retains AS path information for paths in the aggregated address range.
summary-only:Announce only the path after aggregation.

Description
The aggregate-address command sets the IPv4/ipv6 aggregated routing table entries for BGP.

Examples
Configure aggregated address 10.0.0.0/8 and announce only the path after aggregation.

```
Switch(config)#router bgp 1
Switch(config-router)#aggregate-address 10.0.0.0/8 summary-only
Switch(config-router)#
```

bgp always-compare-med

Command

```
bgp always-compare-med
nobgp always-compare-med
```

Mode
BGP configuration mode.

Parameters
None.

Description
The bgp always-compare-med command sets BGP to always compare Multi Exit Discriminator (MED).

Examples

```
#configure-always-compare-med.
Switch(config)#router bgp 1
Switch(config-router)#bgp always-compare-med
Switch(config-router)#
```

bgp bestpath

Command

```
bgp bestpath<as-path ignore | compare-confed-aspath | compare-routerid | dont-compare-originator-id |
med [confed | missing-as-worst | remove- recv-med | remove-send-med]| tie-break-on-age>
nobgp bestpath<as-path ignore | compare-confed-aspath | compare-routerid | dont-compare-originator-id
| med [confed | missing-as-worst | remove-recv-med | remove-send-med]| tie-break-on-age>
```

Mode
BGP configuration mode.

Parameters
as-path ignore: The length of the AS path is not considered when electing the optimal path.
compare-confed-aspath: When electing the optimal path, allow the same external routes to compare the ASPATH path length of the federation, the smaller the ASPATH length within the federation, the higher the path priority.
compare-routerid: When electing the optimal path, allow the same external route to compare the router ID of the path, the smaller the router ID, the higher the priority of the path.

Description
The bgp bestpath command sets the election of the BGP optimal route.
The no bgp bestpath command removes the election of the BGP best route.

Examples

```
#configure-always-compare-med.
Switch(config)#router bgp 1
```

```
Switch(config-router)#bgp always-compare-med
Switch(config-router)#
```

bgp client-to-client reflection

Command

```
bgp client-to-client reflection
nobgp client-to-client reflection
```

Mode

BGP configuration mode.

Parameters

None.

Description

bgp client-to-client reflection This command turns on the inter-client routing reflection function of the device.

Examples

Routing reflection function between clients with open devices.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp client-to-client reflection
Switch(config-router)#
```

bgp cluster-id

Command

```
bgp cluster-id<cluster-id>
nobgp cluster-id<cluster-id>
```

Mode

BGP configuration mode.

Parameters

cluster-id: The cluster identifier of the route reflector, which can be expressed in decimal, with a value range of 0 to 4294967295; it can also be expressed in 32-bit dotted decimal. The value range is 0.0.0.0 to 255.255.255.255.

Description

bgp cluster-id This command configures the cluster identifier of the route reflector.
nobgp cluster-id This command cancels the cluster identifier of the route reflector.

Examples

Set the group identifier of the route reflector 10.0.0.1.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp cluster-id 1.1.1.1
Switch(config-router)#
```

bgp confederation identifier

Command

```
bgp confederation identifier<as-number>
nobgp confederation identifier
```

Mode

BGP configuration mode.

Parameters

as-number:The identifier of the AS federation. Range: 1-65535.

Description

bgp confederation identifier This command configures the identifier of the AS confederation.
nobgp confederation identifier This command cancels the AS confederation identifier.

Examples

Set the AS Alliance identifier to 100.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp confederation identifier 100
Switch(config-router)#
```

bgp confederation peers

Command

```
bgp confederation peers <as-number>
nobgp confederation peers <as-number>
```

Mode

BGP configuration mode.

Parameters

as-number:Members in the alliance AS. range: 1-65535.

Description

bgp confederation peers This command configures a member AS within a confederation.
nobgp confederation peers This command cancels the member AS in the confederation.

Examples

Set the member AS in the alliance to 5.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp confederation peers 5
Switch(config-router)#
```

bgp default ipv4-unicast

Command

```
bgp default ipv4-unicast
nobgp default ipv4-unicast
```

Mode

BGP configuration mode.

Parameters

None.

Description

bgp default ipv4-unicast This command sets the address family to default to IPv4 unicast addresses.
nobgp default ipv4-unicast This command removes the configured default address family.

Examples

Set address family to default to IPv4 unicast address.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp default ipv4-unicast
Switch(config-router)#
```

bgp default local-preference

Command

```
bgp default local-preference<value>
nobgp default local-preference [value]
```

Mode

BGP configuration mode.

Parameters

value: value of the local priority attribute. Range: 0-4294967295, the default local priority value is 100.

Description
bgp default local-preference This command sets the default value of the local-preference attribute.
nobgp default local-preference This command restores the default value of the local-preference attribute.

Examples
Set the default value of the local-preference attribute to 200.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp default local-preferenc 200
Switch(config-router)#
```

bgp deterministic-med

Command

```
bgp deterministic-med
nobgp deterministic-med
```

Mode
BGP configuration mode.

Parameters
None.

Description
bgp deterministic-med This command sets the path priority comparison MED value for peers from the same AS.
nobgp deterministic-med This command sets the path recovery of peers from the same AS to be compared in the order of path reception, with the most recently received path being compared first.

Examples
Set the path priority comparison MED value for peers from the same AS.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp deterministic-med
Switch(config-router)#
```

bgp enforce-first-as

Command

```
bgp enforce-first-as
nobgp enforce-first-as
```

Mode
BGP configuration mode.

Parameters
None.

Description
bgp enforce-first-as This command sets the UPDATE message to reject the first AS_PATH path segment received that is not the AS number configured by the neighbor.
nobgp enforce-first-as This command cancels the setting.

Examples
Set to reject UPDATE messages received for the first AS_PATH path segment that is not the neighbor's configured AS number.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp enforce-first-as
Switch(config-router)#
```

bgp fast-external-failover

Command

```
bgp fast-external-failover
nobgp fast-external-failover
```

Mode

BGP configuration mode.

Parameters

None.

Description

bgp fast-external-failover This command sets the command to quickly close a BGP session connection when the network interface used by the directly connected EBGP peer to establish the connection fails.
nobgp fast-external-failover This command cancels the setting.

Examples

Set the BGP session connection to be closed when the network interface used by the directly connected EBGP peer to establish the connection fails: # Set the BGP session connection to be closed when the network interface used by the directly connected EBGP peer to establish the connection fails.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp fast-external-failover
Switch(config-router)#
```

bgp graceful-restart

Command

```
bgp graceful-restart
nobgp graceful-restart
```

Mode

BGP configuration mode.

Parameters

None.

Description

bgp fast-external-failover This command enables the graceful restart capability of global BGP.
nobgp fast-external-failover This command disables the graceful restart capability of BGP.

Examples

Set the global BGP graceful restart capability.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp graceful-restart
Switch(config-router)#
```

bgp graceful-restart restart-time

Command

```
bgp graceful-restart restart-time <restart-time >
nobgp graceful-restart restart-time
```

Mode

BGP configuration mode.

Parameters

restart-time :GR Restarter expects the GR Helper to be in the same position as the GR Restarter when it restarts. The maximum wait time before a new connection is established is configured to range from 1 to 3600 seconds, with the default being 120 seconds.

Description

bgp graceful-restart restart-time This command sets the restart time force for BGP graceful restart.
nobgp graceful-restart restart-time This command restores the restart time to the default value of 120 seconds.

Examples

Set the restart time for BGP Elegant Restart to 130.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp graceful-restart restart-time 130
Switch(config-router)#
```

bgp graceful-restart stalepath-time

Command

```
bgp graceful-restart stalepath-time<time>
nobgp graceful-restart stalepath-time
```

Mode

BGP configuration mode.

Parameters

time :After restoring the connection to the neighboring GR device, the stale path is still maintained
Maximum time by validity. The configuration range is from 1 to 3600 seconds.

Description

bgp graceful-restart stalepath-time This command sets the time for the secondary device to keep the route valid during a BGP graceful restart.
nobgp graceful-restart stalepath-time This command restores stalepath-time to the default value of 360.

Examples

Set the time for the secondary device to keep the route valid during a BGP graceful restart to 400.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp graceful-restart stalepath-time400
Switch(config-router)#
```

bgp log-neighbor-changes

Command

```
bgp log-neighbor-changes
nobgp log-neighbor-changes
```

Mode

BGP configuration mode.

Parameters

None.

Description

bgp log-neighbor-changes This command enables logging of BGP status changes without opening debug.
nobgp log-neighbor-changes This command disables this feature.

Examples

Set to log BGP state change information without opening debug.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp log-neighbor-changes
Switch(config-router)#
```

bgp router-id

Command

```
bgp router-id<router-id>
nobgp router-id [router-id]
```

Mode
BGP configuration mode.

Parameters
router-id :IP address.

Description
bgp router-id This command sets the device ID-IP address to be used when running the BGP protocol.
nobgp router-id This command restores the default IP address used.

Examples
Set router-id to 1.1.1.1.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp router-id 1.1.1.1
Switch(config-router)#
```

bgp scan-time

Command

```
bgp scan-time<time>
nobgp scan-time [time ]
```

Mode
BGP configuration mode.

Parameters
time :the interval of timed scan; range: 0-60, unit: second, default is 60 seconds.

Description
bgp scan-time This command sets the time interval for the BGP protocol timed scan.
nobgp scan-time This command restores the BGP protocol timed scan interval to 60 seconds.

Examples
Set the BGP protocol timed scan interval to 30 seconds.

```
Switch(config)#router bgp 1
Switch(config-router)#bgp scan-time 30
Switch(config-router)#
```

bgp update-delay

Command

```
bgp update-delay<time>
nobgp update-delay [time ]
```

Mode
BGP configuration mode.

Parameters
time :The maximum delay time in seconds before the BGP Speaker sends its updated routing information, configured from 0 to 3600, default is 120 seconds. The maximum time to wait for EOR messages from all neighbors to be received during a BGP graceful restart. The configuration range is from 1 to 3600 seconds.

Description
bgp update-delay This command sets the maximum delay time before the BGP Speaker sends an update message to its neighbors for the first time.
nobgp update-delay This command removes the configuration of bgp update-delay and restores the initial delay to the default value of 120 seconds.

Examples
Set the maximum delay time before the BGP Speaker sends an update message to its neighbors for the first time to 200 seconds.

```
Switch(config)#router bgp 1
```

```
Switch(config-router)#bgp update-delay 200
Switch(config-router)#
```

clear bgp

Command

```
clear bgp< * | as-number |neighbor-address]> [in | out | soft]
```

Mode

Privilege mode.

Parameters

as-number: Resets the session with all members in the specified AS.
neighbor-address:Reset the session of the specified neighbor.
In: without the parameter soft, resets the peer to establish an actively connected session
Out:without parameter soft, reset this BGP speaker to establish active connection
The session
Soft:Soft reset, and the specified peer to send and receive the routing information are performed soft reset

Description

clear bgp This command resets all address families of BGP.

Examples

```
#Resets for all address families of BGP.
Switch#clear bgp *
```

clear bgp ipv4 unicast dampening

Command

```
clear bgp ipv4 unicast dampening [address [ mask ]]
```

Mode

Privilege mode.

Parameters

address:IP address.
mask:Mask.

Description

clear bgp ipv4 unicast dampening: This command clears the oscillation information and unsuppresses the suppressed routes.

Examples

Clear oscillation information and unsuppress suppressed routes.

```
Switch#clear bgp ipv4 unicast dampening
```

clear bgp ipv4 unicast flap-statistics

Command

```
clear bgp ipv4 unicast flap-statistics [address [ mask ]]
```

Mode

Privilege mode.

Parameters

address:IP address.
mask:Mask.

Description

clear bgp ipv4 unicast flap-statistics: This command clears the route oscillation statistics.

Examples

Clear routing oscillation statistics.

```
Switch#clear bgp ipv4 unicast flap-statistics
```

distance bgp

Command

```
distance bgp<external-distance><internal-distance><local-distance>
no distance bgp<external-distance><internal-distance><local-distance>
```

Mode

BGP configuration mode.

Parameters

external-distance :The administrative distance to learn routes from EBGP peers. Range: 1-255, the default value is 20.
internal-distance : The administrative distance to learn routes from IBGP peers. Range: 1-255, the default value is 200.
local-distance: The administrative distance learned from peers, but considered to exist for routes that can be learned better from IGP, usually these routes are indicated by the networkbackdoor command. Range: 1-.255, default value is 200

Description

distance bgp This command sets different administrative distances for different types of BGP routes.
nodistance bgp This command restores the default administrative distance.

Examples

Set external-distance to 30, internal-distance to 40 and local-distance to 50.

```
Switch(config)#router bgp 1
Switch(config-router)#distance bgp 30 40 50
Switch(config-router)#
```

neighbor activate

Command

```
neighbor [ peer-address | peer-tag ] activate
noneighbor [ peer-address | peer-tag ] activate
```

Mode

BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

Description

neighbor activate This command activates a neighbor or peer group in the current address mode.
noneighbor activate This command restores it to the default value.

Examples

```
#Activate Neighborhood 10.0.0.1.
Switch(config-router)#neighbor 10.0.0.1 remote-as 100
Switch(config-router)#address-family ipv4
Switch(config-router-af)#neighbor 10.0.0.1 activate
Switch(config-router-af)#
```

neighbor advertisement-interval

Command

```
neighbor [ peer-address | peer-tag]advertisement-interval<seconds>
noneighbor [ peer-address | peer-tag]advertise-interval
```

Mode
BGP configuration mode.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
Seconds: The time interval for sending routing updates. Range: 1-600 seconds

Description
neighbor advertisement-interval This command sets the time interval for sending BGP routing updates.
noneighbor advertisement-interval This command restores it to the default value.

Examples
Set the interval for neighbor 1.1.1.1 BGP routing updates to 10 seconds.

```
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
Switch(config-router)#neighbor 1.1.1.1 advertisement-interval 10
Switch(config-router)#
```

neighbor allowas-in

Command

```
neighbor [ peer-address | peer-tag ] allowas-in [number]
noneighbor [ peer-address | peer-tag ]allowas-in
```

Mode
BGP configuration mode, BGP IPv4 address family configuration mode.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
number: the number of times the AS number is allowed to be repeated, the default value is 3, the range of values is
in [1,10].

Description
neighbor allowas-in When configuring a PE, use this command to allow the PE to receive messages that contain duplicate AS numbers with this PE.
noneighbor allowas-in This command restores it to the default value.

Examples
Set the number of messages allowed to be received by neighbor 1.1.1.1 PE that contain a duplicate AS number with this PE to 10.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 allowas-in 10
Switch(config-router)#
```

neighbor default-originate

Command

```
neighbor [ peer-address | peer-tag ]default-originate [route-map <map-tag> ]
noneighbor [ peer-address | peer-tag ]default-originate [route-map <map-tag> ]
```

Mode
BGP configuration mode.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

map-tag:The name of the route map route map name does not exceed 32 characters.

Description

neighbor default-originate This command allows the BGP speaker to advertise the default route to the peer (group).
noneighbor default-originate This command cancels the sending of the default route.

Examples

Set to allow the BGP speaker to advertise the default route to the peer (group).

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
Switch(config-router)#neighbor 1.1.1.1 default-originate
Switch(config-router)#
```

neighbor description

Command

```
neighbor [ peer-address | peer-tag]description<text>
noneighbor [ peer-address | peer-tag ]description
```

Mode

BGP configuration mode.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
text: The text to describe the peer (group). range: up to 80 characters.

Description

The peer (group) specified by neighbor description sets the descriptive statement.
noneighbor description This command cancels the configuration.

Examples

Set the peer (group) descriptive for neighbor 1.1.1.1 to abc.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 descriptionabc
Switch(config-router)#
```

neighbor distribute-list

Command

```
neighbor [ peer-address | peer-tag]distribute-list<acl-number>< in
| out>
noneighbor [ peer-address | peer-tag ]distribute-list<acl-number>< in
| out>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
acl-number: The number of the ACL.
In:ACL applied to the received routing information
Out:ACL applied to the routing information distributed out.

Description

neighbor distribute-list Specifies that when a BGP peer sends and receives routing information, the routing policy is implemented according to the ACL.
noneighbor distribute-list This command cancels the set ACLs.

Examples

When setting the peer (group) of neighbor 1.1.1.1 to receive routing information, the routing policy is implemented for 10 according to the ACL.

```
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
Switch(config-router)#neighbor 1.1.1.1 distribute-list10 in
Switch(config-router)#
```

neighbor filter-list

Command

```
neighbor [ peer-address | peer-tag]filter-list<acl-number>< in
| out>
noneighbor [ peer-address | peer-tag]filter-list<acl-number>< in
| out>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
acl-number: The number of the ACL.
In:ACL applied to the received routing information
Out:ACL applied to the routing information distributed out.

Description

neighbor filter-list sets a route filter to be used when sending and receiving routing information to and from the specified BGP peer.
noneighbor filter-list This command cancels the set filter.

Examples

Set the peer (group) of neighbor 1.1.1.1 to implement route filtering according to ACL for 10 when receiving routing information.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 filter-list10 in
Switch(config-router)#
```

neighbor local-as

Command

```
neighbor [ peer-address | peer-tag]local-as<as-number>
noneighbor [ peer-address | peer-tag]local-as<as-number>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
as-number: The set local AS number. Range: 1 to 4294967295.

Description

The neighbor local-as setting configures a local AS number for a BGP peer, so that the peer device can use the local AS as its RemoteAS to establish a BGP connection with this device.
noneighbor local-as This command removes the configured local AS.

Examples

Set the peer (group) local AS number of neighbor 1.1.1.1.

```
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
Switch(config-router)#neighbor 1.1.1.1 local-as200
Switch(config-router)#
```

neighbor maximum-prefix

Command

```
neighbor [ peer-address | peer-tag ]maximum-prefix<maximum> [ threshold ][warning-only]
noneighbor [ peer-address | peer-tag]maximum-prefix
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
maximum:The upper limit of the entries allowed to receive routing information.
Threshold:Specify the value to start generating warnings and the percentage of the maximum number
warning-only: Instead of terminating the BGP connection when the route information reaches the upper limit, generate a
The log information.

Description

The neighbor maximum-prefix setting limits the number of prefixes received from the specified BGP peer.
noneighbor maximum-prefix This command cancels the set limit.

Examples

Set the limit on the number of peer (group) prefixes for neighbor 1.1.1.1 to 50.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 maximum-prefix50
Switch(config-router)#
```

neighbor next-hop-self

Command

```
neighbor [ peer-address | peer-tag]next-hop-self
noneighbor [ peer-address | peer-tag]next-hop-self
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

Description

neighbor next-hop-self Sets the next hop of the routing information to this BGP speaker when the specified BGP peer distributes routes.
noneighbor next-hop-self This command cancels the setting.

Examples

Set the next hop setting for this BGP speaker when the peer (group) of neighbor 1.1.1.1 distributes routes.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 next-hop-self
Switch(config-router)#
```

neighbor prefix-list

Command

```
neighbor [ peer-address | peer-tag]prefix-list<prefix-list-name>< in
| out>
noneighbor [ peer-address | peer-tag]prefix-list< in| out>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
prefix-list-name:The name of the prefix-list. The prefix list name should be no more than 32 characters.
In:ACL applied to the received routing information
Out:ACL applied to the routing information distributed out.

Description

neighbor prefix-list Set this command to implement routing policies based on the prefix list when the specified BGP peer sends and receives routing information.
noneighbor prefix-list This command cancels the set prefix-list.

Examples

When setting the peer (group) of neighbor 1.1.1.1 to receive routing information, the routing policy is applied according to the prefix list real 10.

```
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
Switch(config-router)#neighbor 1.1.1.1 prefix-list10 in
Switch(config-router)#
```

neighbor remote-as

Command

```
neighbor [ peer-address | peer-tag]remote-as<as-number>
noneighbor [ peer-address | peer-tag ]remote-as<as-number>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
as-number: BGP peer (group) autonomous system number. Range: 1 to 4294967295.

Description

neighbor remote-as This command configures a BGP peer (group).
noneighbor remote-as This command removes the configured peer (group).

Examples

Set the peer (group) of neighbor 1.1.1.1 to 100.

```
Switch(config-router)#neighbor 1.1.1.1 remote-as 100
```

neighbor remove-private-AS

Command

```
neighbor [ peer-address | peer-tag]remove-private-AS
noneighbor [ peer-address | peer-tag]remove-private-AS
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

Description

neighbor remove-private-AS This command removes the private AS number recorded in the AS path attribute of a route sent to the specified EBGP peer.
noneighbor remove-private-AS This command cancels the setting.

Examples

Delete the private AS number recorded in the AS Path attribute of the route of the peer of neighbor 1.1.1.1.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 remove-private-AS
Switch(config-router)#
```

neighbor route-map

Command

```
neighbor [ peer-address | peer-tag]route-map<map-tag>< in
| out>
noneighbor [ peer-address | peer-tag]route-map<map-tag>< in
| out>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
map-tag:The name of the matching rule.
In:ACL applied to the received routing information
Out:ACL applied to the routing information distributed out.

Description

neighbor route-map This command uses route matching for incoming or outgoing routes.
noneighbor route-map This command disables this feature.

Examples

Set the routes received by the peer (group) of neighbor 1.1.1.1 to use route-matching route-map10.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 route-map10 in
Switch(config-router)#
```

neighbor route-reflector-client

Command

```
neighbor [ peer-address | peer-tag]route-reflector-client
noneighbor [ peer-address | peer-tag]route-reflector-client
```

Mode

BGP configuration mode.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

Description

neighbor route-reflector-client This command configures this device as a route reflector and specifies its client.
noneighbor route-reflector-client This command cancels the set client.

Examples

Set the peer (group) route reflector for neighbor 1.1.1.1 and specify its client.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 route-reflector-client
Switch(config-router)#
```

neighbor send-community

Command

```
neighbor [ peer-address | peer-tag ]send-community[ both | standard |
extended ]
noneighbor [ peer-address | peer-tag ]send-community[ both | standard |
extended ]
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
Both: Standard and extended groups are transmitted.
Standard: Only the standard groups are transmitted.
Extended: Transmits only extended groups.

Description

neighbor send-community This command specifies that the group attribute is transmitted to the specified BGP neighbor.
noneighbor send-community This command disables this feature.

Examples

Specifies that the group attribute is transmitted to the specified BGP neighbor 1.1.1.1.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 send-community
Switch(config-router)#
```

neighbor shutdown

Command

```
neighbor [ peer-address | peer-tag]shutdown
noneighbor [ peer-address | peer-tag]shutdown
```

Mode
BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

Description
neighbor shutdown This command shuts down the BGP connection to the specified BGP peer.
noneighbor shutdown This command restarts the BGP peer (group).

Examples
```
#Close the BGP connection to neighbor 1.1.1.1.
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 shutdown
Switch(config-router)#
```

neighbor timers

Command
```
neighbor [ peer-address | peer-tag]timers<keepalive><holdtime>
noneighbor [ peer-address | peer-tag]timers<keepalive><holdtime>
```

Mode
BGP configuration mode.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
Keepalive: the time to send a KEEPALIVE message to the specified BGP peer
Interval. Range: 0-65535 seconds. The default value is 60 seconds.
Holdtime: The time interval to consider the BGP peer still valid. Range: 0-65535 seconds.
The default value is 180 seconds.

Description
neighbor timers This command sets the keepalive and
holdtime Time value.
noneighbor timers This command restores the default value.

Examples
Set neighbor 1.1.1.1's Keepalive to 70 and holdtime to 300.
```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 timers 70 300
Switch(config-router)#
```

neighbor unsuppress-map

Command
```
neighbor [ peer-address | peer-tag]unsuppress-map<map-tag>
noneighbor [ peer-address | peer-tag ]unsuppress-map<map-tag>
```

Mode
BGP configuration mode.

Parameters
peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.

map-tag:The name of the route-map. route map names should be no more than 32 characters.

Description

neighbor unsuppress-map This command allows selective advertisement of routing information previously suppressed by the s aggregate-address command.
noneighbor unsuppress-map This command restores the default configuration.

Examples

Set neighbor 1.1.1.1 to allow selective advertisement of routing information previously suppressed by the aggregate-address command.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 unsuppress-map10
Switch(config-router)#
```

neighbor update-source

Command

```
neighbor [ peer-address | peer-tag]update-source<interface>
noneighbor [ peer-address | peer-tag]update-source<interface>
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
interface:Interface name or interface address.

Description

neighbor update-source This command sets the network interface to be used when establishing a BGP connection.
noneighbor update-source This command restores the automatic matching of the best local interface.

Examples

Set the network interface oh vlan1 to be used when establishing a neighbor 1.1.1.1 BGP connection.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 update-sourcevlan1
Switch(config-router)#
```

neighbor version

Command

```
neighbor [ peer-address | peer-tag]version<number>
noneighbor [ peer-address | peer-tag]version<number>
```

Mode

BGP configuration mode.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
number: version number, the default version number is 4.

Description

neighbor version This command specifies the version number of the BGP protocol used by a particular BGP neighbor.
noneighbor version This command restores the use of the default version number.

Examples

Set the version number of the BGP protocol used by neighbor 1.1.1.1 to 4.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 version 4
Switch(config-router)#
```

neighbor weight

Command

```
neighbor [ peer-address | peer-tag]weight<number>
noneighbor [ peer-address | peer-tag ]weight<number>
```

Mode

BGP configuration mode.

Parameters

peer-address :Specify the address of the peer, which may be an IPv4 address, or
Possibly an IPv6 address.
peer-tag : Specifies the name of the peer group. The peer group name should be no more than 32 characters.
number: the weight value of the neighbor. Value range: 0 - 65535.

Description

The neighbor weight command describes the weight value used for a specific BGP neighbor.
noneighbor weight This command cancels the setting of the neighbor's weight value.

Examples

Set neighbor 1.1.1.1 weight value 100.

```
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 weight100
Switch(config-router)#
```

network

Command

```
network <network-number> mask <mask> [ route-map <map-tag> ] [ backdoor]
nonetwork <network-number> mask <mask> [ route-map] [ backdoor]
```

Mode

BGP configuration mode.

Parameters

network-number:Network number.
mask: The subnet mask.
map-tag:The name of the route-map. route map names should be no more than 32 characters.
Backdoor:This route is a backdoor route.

Description

network This command configures the network information that needs to be announced by this BGP speaker.
nonetwork This command deletes the set network information.

Examples

Set the network information of the announcement 192.168.2.0, subnet mask 255.255.255.0.

```
Switch(config)#router bgp 1
Switch(config-router)#network 192.168.2.0 mask 255.255.255.0
Switch(config-router)#
```

redistribute

Command

```
redistribute<protocol-type> [ route-map <map-tag> ]
noredistribute<protocol-type> [ route-map <map-tag> ]
```

Mode

BGP configuration mode, IPv4 address family configuration mode for BGP, and IPv6 address family configuration mode for BGP.

Parameters

protocol-type:The source protocol type of the route being redistributed.
map-tag: The name of the associated route-map. No route-map is associated by default.

Description

redistribute This command redistributes routing information between other routing protocols and BGP.
noredistribute This command removes the feature and its parameter configuration.

Examples

Introducing OSPF routing.

```
Switch(config)#router bgp 1
Switch(config-router)# redistribute ospf
Switch(config-router)#
```

synchronization

Command

```
synchronization
nosynchronization
```

Mode

BGP configuration mode.

Parameters

None.

Description

synchronization This command starts the synchronization mechanism of BGP and IGP routing information.
nosynchronization This command cancels the synchronization mechanism of BGP and IGP.

Examples

Start the synchronization mechanism for BGP and IGP routing information.

```
Switch(config)#router bgp 1
Switch(config-router)# synchronization
Switch(config-router)#
```

timers bgp

Command>
timers bgp<keepalive><holetime>
notimers bgp<keepalive><holetime>

Mode

BGP configuration mode.

Parameters

keepalive:When sending a KEEPALIVE message to the specified BGP peer
interval. Range: 0-65535 seconds, default is 60 seconds.
holetime: The time interval during which the BGP peer is considered still valid. Range: 0-65535 seconds. Default is 180 seconds

Description
timers bgp This command is used to adjust the network timers of BGP.
nortimers bgp This command restores the default values.

Examples
Set keepalive to 70 seconds and holetime to 220 seconds.

```
Switch(config)#router bgp 1
Switch(config-router)#timers bgp 70 220
Switch(config-router)#
```

View command

show bgp

Command

```
show bgp [community | community-list <community-name> [ exact-match] | dampening dampened-paths |
dampening flap-statistics | filter-list& lt;path-list-number > | inconsistent-as |
prefix<ip-prefix-list-name > | quote-regexp <regexp> | regexp <regexp> | route- map <map-tag> |
neighbors ]
```

Mode
Privilege mode.

Parameters
Community: Displays information about the route with the specified community value.
community-name:community-name is the name of the group list.
exact -match: Exactly match the group value or group list for the routing information.
dampening dampened-paths: Displays information about suppressed routes.
dampening flap-statistics: Displays routing oscillation statistics.
filter-list path-list-number: Displays information about routes that match the filter list. path-list-numbe is the filter-list label number.
inconsistent-as: Displays information about routes with conflicting source ASs.
prefix ip-prefix-list-name: Displays information about routes that match the specified prefix-list filter.
quote-regexp regexp: displays the regular expressions whose AS path attributes match within the specified double quotes
BGP routing information.
regexp regexp: displays the BGP routes whose AS path attributes match the specified regular expression Information.
route-map map-tag: Displays information about routes that meet the specified route-map filtering criteria.
Neighbors: Displays the specified neighbor routing information.

Description
The show bgp command uses information from BGP.

Examples
Display BGP neighbor information.

```
Switch#show bgp neighbors
BGP neighbor is 192.168.0.1, remote AS 1, local AS 1, internal link
BGP version 4, remote router ID 192.168.0.1
BGP state = Established, up for 00:05:00
Last read 00:05:00, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Received 13 messages, 0 notifications, 0 in queue
Sent 16 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 5 seconds
```

```
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
0 accepted prefixes
1 announced prefixes
Connections established 1; dropped 0
Local host: 192.168.0.5, Local port: 179
Foreign host: 192.168.0.1, Foreign port: 56694
Nexthop: 192.168.0.5
Nexthop global: 3ffe:506::5
Nexthop local: fe80::2a7:c1ff:fed1:5581
BGP connection: non shared network
```

show ip bgp

Command

```
show ip bgp[<network>[network-mask] | community | community-list <community-name> [ exact-match] |
dampening dampened-paths | dampening flap-statistics |filter-list<path-list-number > |
inconsistent-as | prefix<ip-prefix-list-name > | quote-regexp < regexp> | regexp <regexp> | route-map
<map-tag> | neighbors ]
```

Mode

Privilege mode.

Parameters

Network: Displays specific routing information in the routing table.
network-mask: Displays the routing information contained in the specified network.
Community: Displays information about the route with the specified community value.
community-name:community-name is the name of the group list.
exact -match: Exactly match the group value or group list for the routing information.
dampening dampened-paths: Displays information about suppressed routes.
dampening flap-statistics: Displays routing oscillation statistics.
filter-list path-list-number: Displays information about routes that match the filter list. path-list-numbe is the filter-list label number.
inconsistent-as: Displays information about routes with conflicting source ASs.
prefix ip-prefix-list-name: Displays information about routes that match the specified prefix-list filter.
quote-regexp regexp: displays the regular expressions whose AS path attributes match within the specified double quotes
BGP routing information.
regexp regexp: displays the BGP routes whose AS path attributes match the specified regular expression Information.
route-map map-tag: Displays information about routes that match the specified route-map filtering criteria.
Neighbors: Displays the specified neighbor routing information.

Description

show ip bgp This command displays unicast routing information in BGP routing information.

Examples

Display BGP routing information.

```
Switch#show ip bgp
BGP table version is 5, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*>i192.168.0.0 192.168.0.5 0 100 0 i
Total number of prefixes 1
Switch#:
```

Debugging commands

debug bgp

Command

```
debug bgp[all | dampening | events | filters | fsm | keepalives | nht | nsm | update [in | out] ]
no debug bgp
```

Mode

Privilege mode.

Parameters

All:Turn on all BGP modulation switches.
Dampening: BGP Dampening modulation switch.
Events: BGP events tuned switch.
filters: BGP filters tuned switch.
Fsm: BGP Finite State Machine tuned switch.
Keepalives: BGP keepalives modulation switch.
Nht: NHT message modulating switch.
Nsm: NSM message modulating switch.
Updates: BGP updates tuned switch.

Description

The debug bgp command is used to turn on the bgp-related debug switch to enable the user to see the bgp-related negotiation process and the messages sent and received.
The no debug bgp command is used to disable the bgp debug switch

Examples

Turn on all debug switches of bgp and display bgp debug information

```
switch#debug bgp
```

CHAPTER 32

VRRP commands

Configuration commands

router vrrp

Command

```
router vrrp <vr-id>
no router vrrp <vr-id>
```

Mode

Global configuration mode.

Parameters

vr-id: virtual router ID, the range of values: 1 to 255.

Description

The router vrrp command is used to create a virtual router and enter vrrp configuration mode.
The no router vrrp command is used to delete a vrrp virtual router.

Examples

Create a virtual router with ID 10 and enter vrrp configuration mode.

```
Switch(config)#router vrrp 10
Switch(config-router)#
#Delete the virtual router with ID 10
Switch(config)#no router vrrp 10
Switch(config)#
```

virtual-interface

Command

```
virtual-interface<if-name>
no virtual- interface
```

Mode

vrrp configuration mode.

Parameters

<if-name>: Interface name.

Description

The virtual-interface command is used to configure the virtual interface of vrrp.
The no virtual-interface command is used to delete the virtual interface of vrrp.

Examples

Configure the virtual interface of the virtual router with ID 10 as vlan1

```
Switch(config)#router vrrp 10
Switch(config-router)#virtual-interface vlan1
```

virtual-ip

Command

```
virtual-ip<ip-address><backup | master>
no virtual-ip
```

Mode
vrrp configuration mode.

Parameters
ip-address: ip address of the virtual router, in dotted decimal format.
Note: The address must be in the same network segment as the actual address of the interface.
backup | master :whether the virtual IP address is the same as the actual IP address, the same as master otherwise it is backup

Description
The virtual-ip command is used to configure the ip address for a virtual router.
The no virtual-ip command is used to delete the ip address configured by the virtual router.

Examples
Configure the virtual router with ID 10 to have a virtual ip address of 192.168.1.1

```
Switch(config)#router vrrp 10
Switch(config-router)#virtual-interface vlan1
Switch(config-router)#virtual-ip 192.168.1.1 backup
#Delete the virtual ip address of the virtual router with ID 10
Switch(config)#router vrrp 10
Switch(config-router)#no virtual-ip
```

advertisement-interval

Command

```
advertisement-interval<interval>
```

Mode
vrrp configuration mode.

Parameters
interval: The time interval for the virtual router to send periodic messages, in seconds, in the range of 1 to 10. The default is 1 second.

Description
The advertisement-interval command is used to configure the interval at which the virtual router as master sends periodic messages.

Examples
Configure the virtual router with ID 10 to have a periodic message interval of 10 seconds: Switch(config)#router vrrp 10

```
Switch(config-router)#advertisement-interval 10
Switch(config-router)#
```

authentication

Command

```
authentication {none | simple-password <password>}
```

Mode
vrrp configuration mode.

Parameters
none: Specifies that vrrp messages do not use authentication.
simple-password <password>: Specify that vrrp uses simple text authentication and configure the authentication code.

Description
The authentication command is used to specify the authentication method and authentication password for vrrp messages.

Examples

```
#The virtual router with configuration ID 10 uses simple text authentication with the password
"pass123".
Switch(config)#router vrrp 10
Switch(config-router)#authentication simple-password pass123
Switch(config-router)#
```

preempt-mode

Command

```
preempt-mode{false | true}
```

Mode

vrrp configuration mode.

Parameters

false: Do not use preemption mode.
true: Use preemption mode.

Description

The preempt-mode command is used to specify whether the vrrp virtual router uses preemption mode. when the preempt mode is true, the party using preemption mode will be the master under equal circumstances. true by default.

Examples

```
#The virtual router with configuration ID 10 does not use preemption mode.
Switch(config)#router vrrp 10
Switch(config-router)#preempt-mode false
Switch(config-router)#
```

priority

Command

```
priority <priority-value>
```

Mode

vrrp configuration mode.

Parameters

priority-value: priority value. The value range is 1 to 255, and the default is 100.

Description

The priority command is used to specify the priority of negotiation messages sent by the vrrp virtual router. Under the same condition, the party with the higher priority becomes the master.

Examples

```
#Configure the virtual router with ID 10 to have a priority of 70.
Switch(config)#router vrrp 10
Switch(config-router)#priority 70
Switch(config-router)#
```

circuit-failover

Command

```
circuit-failover<if-name><priority-value>
no circuit-failover
```

Mode

vrrp configuration mode.

Parameters

if-name: Configure the name of the monitored interface; it can be a Layer 2 port or an aggregation port. UP/DOWN of the interface will trigger the priority change of vrrp's periodic notification messages.
priority-value: priority value. The value range is 1 to 253.

Description

The circuit-failover: command is used to configure the monitoring port for the vrrp circuit-failover function. vrrp's circuit-failover function is used to monitor the interface state of the specified interface to enable dynamic adjustment of the vrrp switch's master-standby relationship. After monitoring an interface down, the local vrrp interface sends an announcement message with the priority of the source priority minus the value of priority-value. The notification message when the interface is UP uses the configured priority, and the dynamic switching of vrrp primary and backup is achieved through priority changes.
The no circuit-failover: command is used to remove the configuration of the monitoring port.

Examples

```
Configure the virtual router with vrid 1 to monitor the interface with ge1/3 priority 10.
Switch(config)#router vrrp 1
Switch(config-vrrp)#circuit-failover ge1/2 10
Switch(config-vrrp)#end
Switch#show vrrp 1
VrId <1>
Admin state is Down
State is Initialize
Virtual IP is unset
Interface is unset
Priority is unset
Advertisement interval is 1 sec
Preempt mode is TRUE
Circuit failover interface ge1/2, Priority Delta 10, Status UP
Switch#
```

disable/enable

Command

```
disable
enable
```

Mode

vrrp configuration mode.

Parameters

None

Description

The disable command is used to disable the vrrp function of the current virtual router.
The enable command is used to enable the vrrp function of the current virtual router.

Examples

```
#Enable the vrrp function of the virtual router with id 10.
Switch(config)#router vrrp 10
Switch(config-router)#virtual-interface vlan1
Switch(config-router)#virtual-ip 192.168.1.1 backup
Switch(config-router)#enable
Switch(config-router)#
#Disable the vrrp function of the virtual router with id 10.
Switch(config)#router vrrp 10
Switch(config-router)#disable
```

View command

show vrrp

Command

```
show vrrp [<vr-id>]
```

Mode

Privilege mode / Normal mode.

Parameters

vr-id: Virtual router ID, the range of values: 1 to 255.

Description

The show vrrp command is used to display the currently configured vrrp and its working status. By default, all vrrp information is displayed.

Examples

View vrrp configuration with virtual router ID 1.

```
Switch#show vrrp 1
VrId <1>
Admin state is Up
State is Backup
Virtual IP is 192.168.0.10 (Not IP owner)
Interface is vlan1
Priority not configured, Current priority is 97
Advertisement interval is 1 sec
Preempt mode is TRUE
Authentication type is none
Circuit failover interface ge1/2, Priority Delta 3, Status DOWN
Switch#
```

Debugging commands

debug vrrp

Command

```
debug vrrp
no debug vrrp
```

Mode

Privilege mode.

Parameters

None.

Description

The debug vrrp command is used to turn on the debug switch of the current vrrp so that users can see the negotiation process and the message sending and receiving of vrrp.
The no debug vrrp command is used to turn off the debug switch of vrrp.

Examples

Turn on the debug switch for vrrp.

```
Switch#debug vrrp
Switch#
```

debug vrrp all

Command

```
debug vrrp all
no debug vrrp all
```

Mode

Privilege mode.

Parameters

None.

Description

The debug vrrp all command is used to turn on all vrrp-related debug switches so that users can see the negotiation process and the messages sent and received by vrrp.
The no debug vrrp all command is used to turn off all vrrp-related debug switches.

Examples

Turn on all debug switches related to vrrp.

```
Switch#debug vrrp all
Switch#
```

debug vrrp events

Command

```
debug vrrp events
no debug vrrp events
```

Mode

Privilege mode.

Parameters

None.

Description

The debug vrrp events command is used to turn on the event debugging switch for vrrp, enabling users to see the negotiation process of vrrp.
The no debug vrrp events command is used to turn off the event debugging switch for vrrp.

Examples

Turn on vrrp's event message debug switch.

```
Switch#debug vrrp events
Switch#
```

debug vrrp packet

Command

```
debug vrrp packet [recv | send]
no debug vrrp packet [recv | send]
```

Mode

Privilege mode.

Parameters

recv: Turn on the receive message debug switch.
send: Turn on the send message debug switch.

Description

The debug vrrp command is used to turn on the debug switch of the current vrrp so that users can see the negotiation process and the message sending and receiving of vrrp.
The no debug vrrp command is used to turn off the debug switch of vrrp.

Examples

Turn on the receive message details debug switch for vrrp.

```
Switch#debug vrrp packet recv
Switch#
```

CHAPTER 33

VLLP commands

Configuration commands

router vllp

router vllp <if-name>
no router vllp <if-name>

Mode
Global configuration mode

Parameters
If-name: The name of the interface on which to start the vllp protocol. The interface can only be a Layer 3 vlan interface.

Description
the router vllp command is used to create a vlan-related vllp process and enter vllp configuration mode.
The no router vllp command is used to delete the vllp process for the specified vlan.

Examples
Start vllp process on vlan8.

```
Switch(config)#router vllp vlan8
Switch(config-vllp)#
```

vllp disable/enable

vllp {enable | disable}

Mode
vllp configuration mode

Parameters
None.

Description
The vllp enable command is used to enable the vllp protocol.
The vllp disable command is used to disable the vllp protocol.
Ex·amples
Start vllp protocol on vlan8.
Switch(config)#router vllp vlan8
Switch(config-vllp)#vllp enable
Switch(config-vllp)#

vllp port

vllp port <if-name>
no vllp port <if-name>

Mode
vllp configuration mode

Parameters
If-name: The name of the Layer 2 interface, which can be a Trunk group. The interface must be within the currently configured vllp vlan.

Description
The vllp port command is used to add a port that participates in the vllp loop calculation, which is empty by default.
The no vllp port command is used to specify that a port no longer participates in the vllp loop calculation.

Examples
Specify that two ports ge1/2 and ge1/2 in vlan4 are involved in the loop calculation.

```
Switch#show vlan 4
VLAN Name State Member ports ([u]-Untagged, [t]-Tagged)
---- -------- --------- ------------------------------------------------
4 vlan4 active [t]ge1/2 [t]ge1/3
Switch#config terminal
Switch(config)#router vllp vlan4
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)#
```

vllp priority

vllp priority <priority-value>
no vllp priority [<priority-value >]

Mode
vllp configuration mode

Parameters
priority-value: priority value, the range is 1 to 255, the default value is 100.

Description
The vllp priority command is used to configure the priority of vlan when negotiating vllp with other switches.
The no vllp priority command is used to remove the priority configuration of vlan for vllp negotiation and restore it to the default value.

Examples
Configure vlan4 with a vllp priority of 108.

```
Switch(config)#router vllp vlan4
Switch(config-vllp)#vllp priority 108
Switch(config-vllp)#
```

vllp query-interval

vllp query-interval <interval-value>
no vllp query-interval [<interval -value >]

Mode
vllp configuration mode

Parameters
interval-value: the time interval for sending vllp protocol query messages, the range is 1 to 255, the default value is 5 seconds.

Description
The vllp query-interval command is used to configure the time interval for sending vllp query messages when this end is the sending end.
The no vllp query-interval command is used to remove the configuration of the time interval for sending vllp query messages from this end and restore it to the default value.

Examples
Configure vlan4 to send vllp query messages at an interval of 10 seconds when acting as a sender.

```
Switch(config)#router vllp vlan4
Switch(config-vllp)#vllp query-interval 10
Switch(config-vllp)#
```

vllp dependency

Command

```
vllp dependency<if-name>
no vllp dependency<if-name>
```

Mode

vllp configuration mode

Parameters

if-name: Layer 3 vlan interface name.

Description

The vllp dependency command is used to configure dependent VLANs.
The no vllp dependency command is used to remove the dependent VLAN.

Examples

Configure vlan2 as a dependent VLAN for vlan1 VLLP devices.

```
switch(config)#router vllp vlan1
switch(config-vllp)#vllp dependency vlan2
switch(config-vllp)#
```

View command

show vllp

show vllp [<if-name>]

Mode

Normal mode / Privilege mode

Parameters

If-name: The name of the Layer 3 vlan interface.

Description

The show vllp command is used to display an interface configured with the vllp protocol, including the vllp status and parameters of the interface. The link status, STP status, and port mapping of the vllp ports added to the vllp port list are also included when displaying vllp information for the specified vlan.

Examples

View information about the interfaces on the current switch with vllp configured.

```
Switch#show vllp
VLLP Equipment List:
IF: vlan1 Index: 3
Instance: 1
Status: Sender
Priority: 100
Main port: 2006
Timer interval:
local query: 5s
remote query: 5s
protocol query: 5s
interrupt: 25s
Query timer: 00:00:05
Dependency vlan:
Switch#
```

show vllp map

show vllp map

Mode
Normal mode / Privilege mode

Parameters
None.

Description
The show vllp map command is used to display the mapping of vllp ports in each vlan where the vllp protocol is currently configured.

Examples
View the mapping of each vllp interface on the current switch.

```
Switch#show vllp map
Mapping table:
vlan1 name pid status map
ge1/6 2006 Forward 2010
ge1/1 2001 Disable 0
Switch#
```

show debugging vllp

show debugging vllp

Mode
Normal mode / Privilege mode

Parameters
None.

Description
The show debugging vllp command is used to display the current open status of the vllp debug switch.

Examples
Check which vllp debug switches are currently turned on.

```
Switch>show debugging vllp
VLLP debugging status:
VLLP efsm debugging is on
Switch>
```

Debugging commands

debug vllp

debug vllp
no debug vllp

Mode
Privilege mode

Parameters
None.

Description
The debug vllp command is used to turn on all vllp-related debug switches, enabling the user to observe state changes, message sending and receiving, etc. in vllp negotiation.
The no debug vll command is used to turn off all vllp-related debug switches.

Examples

Turn on the vllp debug switch.

```
Switch#debug vllp
Switch#show debug vllp
VLLP debugging status:
VLLP packet receive debugging is on
VLLP packet send debugging is on
VLLP event debugging is on
VLLP efsm debugging is on
VLLP pfsm debugging is on
Switch#
```

debug vllp all

debug vllp all
no debug vllp all

Mode

Privilege mode

Parameters

None.

Description

The debug vllp all command is used to turn on all vllp-related debug switches, the same as the command debug vllp.
The no debug vllp all command is used to turn off all vllp-related debug switches, the same as the command no debug vllp.

Examples

Turn on all debug switches related to vllp.

```
Switch#debug vllp all
Switch#show debug vllp
VLLP debugging status:
VLLP packet receive debugging is on
VLLP packet send debugging is on
VLLP event debugging is on
VLLP efsm debugging is on
VLLP pfsm debugging is on
Switch#
```

debug vllp events

debug vllp events
no debug vllp events

Mode

Privilege mode

Parameters

None.

Description

debug vllp event: used to turn on the vllp event debug switch.
no debug vllp events: Used to disable the vllp events debug switch.

Examples

Turn on vllp-related event debugging switches.

```
Switch#debug vllp events
Switch#log dis
Switch#
2007/04/12 18:55:03 Informational: VLLP:EVENT: QT expires
```

```
2007/04/12 18:55:08 Informational: VLLP:EVENT: QT expires
Switch#
```

debug vllp packet

debug vllp packet [recv | send]
no debug vllp packet [recv | send]

Mode
Privilege mode

Parameters
recv: the received message, with this parameter only the debugging information of the received message is displayed.
send: the message sent, with this parameter only the debugging information of the sent message is displayed.

Description
The debug vllp packet command is used to turn on the debug switch for sending and receiving vllp packets, which allows the user to observe the sending and receiving of vllp protocol packets on the local machine.
The no debug vllp packet command is used to turn off the debug switch for sending and receiving vllp packets.

Examples
Turn on the debug switch for vllp protocol sending messages, and observe the protocol messages sent.

```
Switch#debug vllp pack send
Switch#log dis
Switch#
2006/12/03 19:21:30 Informational: VLLP:SEND: ge1/11 send lq
2006/12/03 19:21:30 Informational: VLLP:SEND:
Ver: 1
Type: 1
Port1: 2203
Prio: 100
QT: 5
Main: 2203
Reserved: 0
Port2: 2203
Link: 1
STP: 3
2006/12/03 19:21:30 Informational: VLLP:EVENT: send packet
2006/12/03 19:21:30 Informational: VLLP:SEND:
des_mac: 00:09:ca:ff:ff:ff
src_mac: 00:00:00:00:00:02
port_id: 2203
vlan_id: 3
data: 01 01 08 9b 64 05 08 9b 00 00 00 00 08 9b 01 03
2006/12/03 19:21:30 Informational: VLLP:SEND: ge1/9 send lq
2006/12/03 19:21:30 Informational: VLLP:SEND:
Ver: 1
Type: 1
Port1: 2201
Prio: 100
QT: 5
Main: 2203
Reserved: 0
Port2: 2201
Link: 1
STP: 2
2006/12/03 19:21:30 Informational: VLLP:EVENT: send packet
2006/12/03 19:21:30 Informational: VLLP:SEND:
des_mac: 00:09:ca:ff:ff:ff
```

```
src_mac: 00:00:00:00:00:02
port_id: 2201
vlan_id: 3
data: 01 01 08 99 64 05 08 9b 00 00 00 00 08 99 01 02
Switch#
```

debug vllp efsm

debug vllp efsm [detail]
no debug vllp efsm

Mode
Privilege mode

Parameters
detail: Adding this parameter will display detailed debugging information related to efsm.

Description
The debug vllp efsm command is used to turn on the device vllp state machine debug switch to be able to observe the device vllp state change information.
The no debug vllp efsm command is used to turn off the vllp device status debug switch.

Examples
Open vllp.

```
Switch#debug vllp efsm detail
Switch#log dis
Switch#
2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-QueryTimer
2006/12/03 19:24:10 Informational: VLLP:EFSM: Update QT 5s
2006/12/03 19:24:10 Informational: VLLP:EFSM: Update IT 25s
2006/12/03 19:24:10 Informational: VLLP:EFSM: Query timer re-on 5s
2006/12/03 19:24:10 Informational: VLLP:EFSM: PFSM event: SendLQ
2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-RecvLA
2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-RecvLA
Switch#
```

debug vllp pfsm

debug vllp pfsm [detail]
no debug vllp pfsm

Mode
Privilege mode

Parameters
detail: Adding this parameter will display detailed debugging information related to pfsm.

Description
The debug vllp pfsm command is used to turn on the vllp port state machine debug switch;
The no debug vllp pfsm command is used to turn off the vllp port state machine debug switch.

Examples
Open vllp.

```
Switch#debug vllp pfsm detail
Switch#log dis
Switch#
2006/12/03 19:23:10 Informational: VLLP:PFSM:ge1/11:Forward-SendLQ[Sender]
2006/12/03 19:23:10 Informational: VLLP:PFSM: Send LQ
2006/12/03 19:23:10 Informational: VLLP:PFSM:ge1/9:Block-SendLQ[Sender]
2006/12/03 19:23:10 Informational: VLLP:PFSM: Send LQ
2006/12/03 19:23:10 Informational: VLLP:PFSM:ge1/11:Forward-RecvLA[Sender]
2006/12/03 19:23:10 Informational: VLLP:PFSM: Set mapping port 2265
```

```
2006/12/03 19:23:10 Informational: VLLP:PFSM: Port interrupt timer on 25s
2006/12/03 19:23:10 Informational: VLLP:PFSM:ge1/9:Block-RecvLA[Sender]
2006/12/03 19:23:10 Informational: VLLP:PFSM: Set mapping port 2267
2006/12/03 19:23:10 Informational: VLLP:PFSM: Port interrupt timer re-on 25s
```

CHAPTER 34

Policy Routing Commands

Configuration commands

policy route

Command

```
policy route<group-id><source-ip><dest-ip><next-ip>
no policy route<group-id>
```

Mode

Global configuration mode

Parameters

group-id: Policy group number, in the range <1-100>.
source-ip: source IP, with three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
wildcard: Determines which bits need to be matched, '0' means they need to be matched, '1' means they don't need to be matched.
dest-ip: Destination IP address. There are three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
next-ip: next-hop IP address

Description

The policy route command configures a policy route, specifying the source IP address, destination IP address, and next-hop IP address.
The no policy route command removes a policy route

Examples

Configure the source IP address as 192.168.1.10 and the destination IP address as 200.0.0.1 to forward data from the next hop as 192.168.2.2.

```
Switch(config)#policy route 3 host 192.168.1.10 host 200.0.0.1 192.168.2.2
Switch(config)#
```

policy route insert

Command

```
policy route insert<group-id><source-ip><dest-ip><next-ip> before <group-id2>
```

Mode

Global configuration mode

Parameters

group-id: Policy group number, in the range <1-100>.
source-ip: source IP, with three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

wildcard: Determines which bits need to be matched, '0' means they need to be matched, '1' means they don't need to be matched.
dest-ip: Destination IP address. There are three input methods.
1) A.B.C.D wildcard can control IP addresses from one network segment.
2) any is equivalent to A.B.C.D 255.255.255.255
3) host A.B.C.D is equivalent to A.B.C.D 0.0.0.0
next-ip: next-hop IP address
group-id2: Policy group number, range <1-100>.

Description
Inserts a new policy route before the original policy route, specifying the source IP address, destination IP address, and next-hop IP address and the location of the insertion.

Examples
insert a policy route before policy route group 2, the source IP address is 192.168.3.10 the destination IP address is 100.0.0.1 data forwarded from the next hop for 192.168.3.2.

```
Switch(config)#policy route insert4 host 192.168.3.10 host 100.0.0.1 192.168.3.2 before 2
Switch(config)#
```

policy route move

Command

```
policy route move<group-id1>{ after | before } <group-id2>
```

Mode
Global configuration mode

Parameters
group-id1: Policy group number, range <1-100>.
group-id2: policy group number, range <1-100>

Description
Moves the location of a policy route.

Examples

```
#Move to policy route group 2 before policy route 1
Switch(config)#policy route move 2 before 1
Switch(config)#
```

View command

show policy route

Command

```
show policy route
```

Mode
Privilege mode / Normal mode.

Parameters
None

Description
Show show policy route is to view information about the policy routes that have been configured.

Examples

```
#Display policy routing information
Switch#show policy route
Policy route information:
Group id:2 Source IP: 1.1.1.1/0.0.255.255 Destination IP: 0.0.0.0/255.255.255.255 nexthop ip
address:1.1.1.1
```

```
Group id:1 Source IP: 0.0.0.0/255.255.255.255 Destination IP: 1.1.1.1/0.0.0.0 nexthop ip
address:192.168.20.100
```

CHAPTER 35

System log commands

General Logging Commands

debug ip

Command

```
debug ip [all | arp | icmp | tcp | udp]
no debug ip [all | arp | icmp | tcp | udp]
```

Mode

Privilege mode.

Parameters

all: debug all ip, arp, icmp, udp, tcp and other protocol packets. Parse important fields of IP packet headers, including protocol type, packet length and layer 4 messages, such as port number, etc.
arp: debug arp protocol packets, can parse whether it is ARP request or response, can parse ARP content, sender IP and receiver MAC address information, etc.
icmp: debug the sending and receiving of icmp protocol data messages. This command mainly parses the source and destination addresses of packet headers.
tcp: debug the transport layer protocol TCP packets sent and received, you can see the packet window size, should
Use the layer port and message size as well as the source and destination addresses.
udp: debug the packets sent and received for the transport layer protocol udp, you can see the application layer port and message size as well as the source and destination addresses of sent and received packets.

Description

The debug ip command is used to turn on the debug switch associated with messages encapsulated with the ip header, enabling the user to see the message sent and received for the specified type of ip message.
The no debug ip command disables the corresponding ip message debug switch.

Examples

Turn on the debug switch for icmp messages.

```
Switch#debug ip icmp
Switch#
```

log stdout

Command

```
log stdout
no log stdout
```

Mode

Privilege mode.

Parameters

None.

Description

The log stdout command is used to open the terminal to display log information in real time

Examples

```
#Open log output
Switch(config)#log stdout
Switch(config)#
```

log trap

Command

```
log trap <[alerts | critical | debugging | emergencies | errors | informational | notifications |
warnings]>
no log trap
```

Mode

Privilege mode.

Parameters

None.

Description

The log trap command is used to set the log level

Examples

Set log level to warnings

```
Switch(config)#log trap warnings
Switch(config)#
```

no debug all

Command

```
no debug all
```

Mode

Privilege mode.

Parameters

None.

Description

The no debug all command is used to turn off all open debug switches.

Examples

Turn off all open debug switches.

```
Switch#no debug all
Switch#
```

show debug ging

Command

```
show debugging [dhcp snooping |erps | igmp snooping | ip | mstp | rip ]
```

Mode

Privilege mode / Normal mode.

Parameters

dhcp snooping: dhcp related debug switch.
erps: The debug switch associated with erps.
Igmp snooping: The relevant debug switch for igmp snooping.
ip: The debug switch associated with ip.
mstp: mstp's related debug switch.
rip: rip's associated debug switch.

Description

The show debug command is used to see which debug switches are currently turned on.

Examples

View debug switch information.

```
Switch#show debugging
```

```
IP debugging status:
RIP debugging status:
MSTP debugging status:
IGMP SNOOPING debugging status:
erps debugging status:
DHCP Snooping debugging status:
Switch#:
```

show log

Command

```
show log
```

Mode

Privilege mode / Normal mode.

Parameters

None.

Description

The show log command is used to display the log information in the log table.

Examples

Display log information.

```
Switch#show log
log file is empty!
Switch#
```

syslog command

syslog open

Command

```
syslog open <server-ip>
```

Mode

Global configuration mode.

Parameters

server-ip: is the server IP address.

Description

Open the syslog protocol.

Examples

```
#Open syslog protocol, the server IP address is 192.168.0.204
Switch(config)#syslog open 192.168.0.204
Switch(config)#
```

syslog close

Command

```
syslog close
```

Mode

Global configuration mode.

Parameters

None.

Description

Close the syslog protocol.

Examples

```
#close the syslog protocol.
Switch(config)#syslog close
Switch(config)#
```

log syslog

Command

```
log syslog
```

Mode

Global configuration mode.

Parameters

None.

Description

The log syslog command is used to open syslog log information.

Examples

```
#Open syslog log messages.
Switch(config)#log syslog
Switch(config)#
```

show syslog

Command

```
show syslog
```

Mode

Privilege mode / Normal mode.

Parameters

None

Description

Display syslog configuration information.

Examples

Display syslog configuration information.

```
Switch#show syslog
Syslog is opened!
server ip address: 192.168.0.204
udp destination port: 515
severity level: debugging
local device name: Switch
```

CHAPTER 36

IPv6 Commands

IPv6 configuration commands

ipv6 address

Command

```
[no] ipv6 address <ipv6-address>/<prefix-length>
```

Mode

vlanif configuration mode.

Parameters

ipv6-address:ipv6 address, for example: 3000::1/64.
prefix-length: the number of bits of the mask, from 0 to 128.

Description

Used to configure IPV6 addresses. The local link address is automatically configured when the interface is UP. Global unicast addresses need to be configured manually.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 address 2000::1/64
Switch(config-vlan1)#
```

ipv6 nd send-ra

Command

```
[no] ipv6 ndsend-ra
```

Mode

vlanif configuration mode.

Parameters

None.

Description

Used to enable the IPV6 send RA messages function. By default, RA messages are inhibited from being sent.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd send-ra
Switch(config-vlan1)#
```

ipv6 nd cur-hop-limit

Command

```
[no] ipv6 nd cur-hop-limit<hop-number>
```

Mode

vlanif configuration mode.

Parameters

hop-number: hop limit, take the value 0-255. By default, the router publish hop limit is 64 hops

Description
Used to configure IPV6 addresses. The local link address is automatically configured when the interface is UP. Global unicast addresses need to be configured manually.

Examples
```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd cur-hop-limit 2000::1/64
Switch(config-vlan1)#
```

ipv6 nd max-ra-interval

Command
```
[no] ipv6 nd max-ra-interval <value>
```

Mode
vlanif configuration mode.

Parameters
value: the maximum interval for sending RA messages, takes the value 4-1800. the default maximum interval for RA messages is 600 seconds

Description
Used to configure the maximum interval between IPV6 sending RAs.

Examples
```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd max-ra-interval 1800
Switch(config-vlan1)#
```

ipv6 nd min-ra-interval

Command
```
[no] ipv6 nd min-ra-interval <value>
```

Mode
vlanif configuration mode.

Parameters
value:Minimum interval for sending RA messages, takes the value 4-1350. the default minimum interval for RA messages is 198 seconds

Description
Used to configure the minimum interval for IPV6 to send RA.

Examples
```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd min-ra-interval 1000
Switch(config-vlan1)#
```

ipv6 nd prefix

Command
```
[no] ipv6 nd prefix <address-prefix>
```

Mode
vlanif configuration mode.

Parameters
address-prefi: address prefix information, e.g. :3000::/64

Description
Used to configure IPV6 address prefix information.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd prefix 2000::/64
Switch(config-vlan1)#
```

ipv6 nd managed-config-flag

Command

```
[no] ipv6 nd managed-config-flag
```

Mode

vlanif configuration mode.

Parameters

None.

Description

Used to configure the IPV6 managed address flag bit. By default, the managed address flag bit is 0, i.e., the host acquires an IPv6 address through stateless auto-configuration.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)# ipv6 nd managed-config-flag
Switch(config-vlan1)#
```

ipv6 nd other-config-flag

Command

```
[no] ipv6 nd other-config-flag
```

Mode

vlanif configuration mode.

Parameters

None.

Description

Set the other configuration flag bit to 1. By default, the other configuration flag bit is 0, i.e., the host obtains other information through stateless auto-configuration.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)# ipv6 nd other-config-flag
Switch(config-vlan1)#
```

ipv6 nd ra-lifetime

Command

```
[no] ipv6 nd ra-lifetime <value>
```

Mode

vlanif configuration mode.

Parameters

value: survival time, takes the value 0-9000s.

Description

Set the router survival time in RA messages. The default is 1800s.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)# ipv6 nd ra-lifetime2000
Switch(config-vlan1)#
```

ipv6 nd retrans-timer

Command

```
[no] ipv6 nd retrans-timer <value>
```

Mode

vlanif configuration mode.

Parameters

value: RA retransmission interval, takes the value 0-4294967295ms.

Description

Set the retransmission interval in RA messages. Default 0.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)# ipv6 nd retrans-timer 100
Switch(config-vlan1)#
```

ipv6 nd reachable-time

Command

```
[no] ipv6 nd reachable-time <value>
```

Mode

vlanif configuration mode.

Parameters

value: RA reach time, take the value 0-3600000ms.

Description

Set the reachable time in RA messages. Default 0.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)# ipv6 nd reachable-time 100
Switch(config-vlan1)#
```

ipv6 nd link-mtu

Command

```
[no] ipv6 nd link-mtu <value>
```

Mode

vlanif configuration mode.

Parameters

value:The size of the MTU value, take the value 1280-1500.

Description

Used to configure the size of the MTU in IPV6 RA messages, default is 0.

Examples

```
Switch#(config)#interface vlan1
Switch(config-vlan1)#ipv6 nd link-mtu1345
Switch(config-vlan1)#
```

ipv6 route

Command

```
[no] ipv6 route<ipv6-des/prefix-length>{<nest-hop>|<if-name>} [distance]
```

Mode
Global configuration mode.

Parameters
ipv6-des/prefix-length:ipv6 target segment, for example: 3000::/64.
nest-hop: next-hop ipv6 address.
ifname:Next-hop vlanif interface.
distance: the administrative distance of the route, takes the value 1-255, default 1.

Description
Used to configure IPV6 static routes.

Examples
```
Switch#(config)#
Switch(config)#ipv6route 3000::/64 2000::2 100
Switch(config)#
```

ping6

Command
```
ping6<ipv6-address> [-c<count> | -h<hoplimit> | -s<packetsize> | -w <timeout>]
```

Mode
Privilege mode

Parameters
ipv6-address: The destination IP address.
-c: The number of requests sent.
-h: Set the number of hops.
-s: ping6 packet size, default 56.
-w: The timeout period in seconds to wait for each response.

Description
ping6 is a network debugging tool to test whether another host is reachable. Simple applications just enter the IPv6 address of the target host; if you use ping6 as a diagnostic tool, you can enter more detailed parameters.

Examples
Send request packet to host 2000::2.
```
Switch#ping62000::2
```

telnet6

Command
```
telnet6 <ipv6-address>
```

Mode
Privilege Mode

Parameters
ipv6-address: The IPv6 address of the target device.

Description
Remote access to other devices via Telnet6 client can be forced out by pressing the CTRL+C key combination.

Examples
Login to the device with remote IP 2000::2.
```
Switch#telnet2000::2
```

IPv6 display commands

show ipv6 interface

Command

```
show ipv6 interface brief
```

Mode

Privilege mode

Parameters

None.

Description

View ipv6 interface information.

Examples

```
Switch#show ipv6 interface brief
vlan1 [up/up]
2000::1
fe80::209:aff:fe22:2312
vlan2 [up/up]
fe80::209:aff:fe22:2312
ge1/1 [up/up]
unassigned
ge1/2 [up/up]
unassigned
ge1/3 [up/up]
unassigned
ge1/4 [up/down]
......
Switch#
```

show ipv6 route

Command

```
show ipv6 route [<network>]
```

Mode

Privilege Mode / Normal Mode

Parameters

Default parameter: Display the routes that are active in the current routing table.
network: Specifies to display the routes of the associated network, expressed in hexadecimal or address prefix/mask form.

Description

The show ipv6 route command is used to display ipv6 routing information. The content includes destination address, mask length, protocol, priority, weight, next hop, and output interface.

Examples

```
#Display the currently used ipv6 routes
Switch#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
Timers: Uptime
C 2000::/64 via ::, vlan1, 31w5d13h
S 3000::/64 [1/0] via 2000::28, vlan1, 31w5d13h
C fe80::/64 via ::, vlan1, 31w5d13h
```

```
Switch#
#Display routes for the specified network
Switch#Switch#show ipv6 route 3000::
Routing entry for 3000::/64
Known via "static", distance 1, metric 0, best
Last update 31w5d13h ago
* via 2000::28, vlan1
Switch#
```

show ipv6 route database

Command

```
show ipv6 route database
```

Mode

Privilege Mode / Normal Mode

Parameters

Default parameter: Display all routes in the routing table, including active and inactive routes.

Description

The show ipv6 routedatabase command is used for the entire routing information in the routing table, including inactive routes.

Examples

Show all routes

```
Switch#show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime
C*> 2000::/64 via ::, vlan1, 31w5d14h
S*> 3000::/22 [1/0] via ::, vlan1, 02:34:26
S*> 3000::/64 [1/0] via 2000::28, vlan1, 31w5d14h
C* fe80::/64 via ::, vlan2, 31w5d14h
C*> fe80::/64 via ::, vlan1, 31w5d14h
Switch#
```

IPv6 debugging commands

debug ipv6

Command

```
[no] debug ipv6 [recv| send]
```

Mode

Privilege mode

Parameters

None.

Description

The debug ipv6 command is used to turn on debugging information for ipv6 and is used with the log display command.

Examples

```
Switch#debug ipv6recv
```

debug ipv6 icmp6

Command

```
[no] debug ipv6 icmp6[recv| send]
```

Mode

Privilege mode

Parameters

None.

Description

The debug ipv6 icmp6 command is used to open the debugging information of icmp6, and log display command a
Same use.

Examples

```
Switch#debug ipv6 icmp6 recv
```

CHAPTER 37

MLDsnooping command

MLDsnooping configuration commands

Ipv6mld snooping

Command

```
Ipv6mld snooping
no ipv6mld snooping
```

Mode

Global configuration mode

Parameters

None

Description

The Ipv6mld snooping command is used to start the mld snooping function for all vlan.
The no ipv6mld snooping command disables the mld snooping function for all vlan.

Examples

```
None.
```

ipv6mld snooping fast-leave

Command

```
ipv6mld snooping fast-leave vlan <vlan-id>
no ipv6mld snooping fast-leave vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

vlan-id: The vlan number to start the immediate departure.

Description

Start the mld immediate leave function for a vlan.
The no command disables the mld immediate leave feature for a vlan.

Examples

Start multicast members of vlan2 to immediately leave the function.

```
Switch(config)# ipv6mld snooping fast-leave vlan 2
Switch(config)#
```

ipv6mld snooping fast-leave-timeout

Command

```
ipv6mld snooping fast-leave-timeout <interval> vlan <vlan-id>
no ipv6mld snooping fast-leave-timeout vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

interval: delay time, in ms, unlimited range. The default is 300000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description

Set the multicast member of a vlan to leave the delay time immediately and wait for the time specified by interval before removing the member after receiving the leave packet.
The no command cancels the immediate leave delay setting, and the interval restores the default value.

Examples

Configure vlan1 to delete a multicast member as soon as it receives a leave packet from that member.

```
Switch(config)# ipv6mld snooping fast-leave vlan 1
Switch(config)# ipv6mld snooping fast-leave-timeout 0 vlan 1
Switch(config)#
```

ipv6mld snooping group-membership-timeout

Command

```
ipv6mld snooping group-membership-timeout <interval> vlan <vlan-id>
no i ipv6mld snooping group-membership-timeout vlan <vlan-id>
```

Mode

Global configuration mode

Parameters

interval: member survival time, in ms, range is unlimited. The default is 400000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description

Configure the survival time of multicast groups that join after receiving a REPORT packet.
The no command cancels the configuration of member survival time and restores the default value.

Examples

Configure vlan2 with a multicast membership survival time of 600 seconds.

```
Switch(config)# ipv6mld snooping group-membership-timeout 600000 vlan 2
Switch(config)#
```

ipv6mld snooping mrouter

Command

```
ipv6mld snooping mrouter vlan <vlan-id>
no ipv6mld snooping mrouter vlan <vlan-id>
```

Mode

Interface configuration mode

Parameters

vlan-id: The vlan number to which the interface belongs.

Description

Configure the query port to which all other ports will forward any multicast join-leave packets they receive; the port will join the multicast group.
The no command removes the configured query port.

Examples

Configure port ge1/1 as a query port for vlan2.

```
Switch(config-ge1/1)# ipv6mld snooping mrouter vlan 2
Switch(config-ge1/1)#
```

ipv6 mld snooping query-membership-timeout

Command

```
ipv6mld snooping query-membership-timeout <interval> vlan <vlan-id>
no ipv6mld snooping query-membership-timeout vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
interval: the survival time of the query port, in ms, range 60000-300000ms. default 300000 ms.
vlan-id: The vlan number of the configured vlan, range 1-4094.

Description
Configure the survival time of the query group joined after receiving a QUERY packet.
The no command cancels the configuration of the query group survival time and restores the default value.

Examples
Configure vlan2 to query the port for 600 seconds.

```
Switch(config)# ipv6mld snooping query-membership-timeout 600000 vlan 2
Switch(config)#
```

ipv6mld snooping vlan

Command

```
ipv6mld snooping vlan <vlan-id>
no ipv6mld snooping vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
vlan-id: vlan number.

Description
To start the mld snooping function of a vlan, you must first execute ipv6mld snooping before you can configure the mld snooping function of a vlan.
The no command disables the ipv6mld snooping function for a vlan.

Examples
Disable mld snooping for vlan3 and turn on ipv6mld snooping for other vlan.

```
Switch(config)#
Switch(config)#no ipv6mld snooping vlan 3
Switch(config)#
```

ipv6mld snooping querier vlan

Command

```
ipv6mld snooping querier vlan <vlan-id>
no ipv6mld snooping querier vlan <vlan-id>
```

Mode
Global configuration mode

Parameters
vlan-id: vlan number.

Description
To start the mld snooping querier function for a vlan, you must execute ipv6mld snooping before you can configure the mld snooping querier function for a vlan.
The no command disables the ipv6mld snooping querier function for a vlan.

Examples
Disable the mld snoopingquerier function for vlan3.

```
Switch(config)#
Switch(config)#no ipv6mld snooping querier vlan 3
Switch(config)#
```

MLDsnooping view command

show ipv6mld snooping

Command

```
show ipv6mld snooping [fast-leave [vlan <vlan-id>] | fast-leave-timeout [vlan <vlan-id>] |
forwarding-table | group-membership- timeout [vlan <vlan-id>] | interface [vlan <vlan-id>] |
query-membership-timeout [vlan <vlan-id>] | vlan <vlan-id> ]
```

Mode

Normal mode / Privilege mode

Parameters

fast-leave: Displays the opening of the leave-now feature.
vlan <vlan-id>: Displays the configuration of the specified vlan.
fast-leave-timeout: Displays the configuration of the immediate leave delay time.
forwarding-table: Displays the multicast forwarding table, including the multicast group and corresponding vlan and port.
group-membership-timeout: Displays the group membership survival time configuration.
interface: Shows the relationship between the available ports and vlan.
query-membership-timeout: Displays the query group survival time configuration.
vlan: Displays the mld snooping configuration for the specified vlan.

Description

Display the ipv6mld snooping configuration.

Examples

Show ipv6mld snooping configuration for vlan1.

```
Switch #show ipv6 mld snooping vlan 1
MLD Snooping is globally enabled
Bridge 1: VLAN 1
MLD Snooping is enabled
MLD Snooping fast-leave-timeout is 300000 ms
MLD snooping query membership timeout is 300000 ms
MLD snooping group membership timeout is 400000 ms
Switch #
```

show ipv6mld snooping age-table

Command

```
show ipv6 mld snooping age-table { group-membership | query-membership}
```

Mode

Normal mode / Privilege mode

Parameters

group-membership: Displays the age time of the member group.
query-membership: Display the age time of the query group.

Description

Displays the age time and the port where the multicast group is located.

Examples

```
#Display the age time of the member group.
Switch#show ipv6 mld snooping age-table group-membership
VLAN Address Port Seconds
2 ff18:0000:0000:0000:0000:0000:0000:0001 ge1/24 70000 ms
2 ff18:0000:0000:0000:0000:0000:0000:0002 ge1/24 70000 ms
2 ff18:0000:0000:0000:0000:0000:0000:0003 ge1/24 70000 ms
```

```
2 ff18:0000:0000:0000:0000:0000:0000:0004 ge1/24 70000ms
Switch#
```

show ipv6 mld snooping mrouter

Command

```
show ipv6 mld snooping mrouter [interface <if-name> | vlan <vlan-id>]
```

Mode

Normal mode / Privilege mode

Parameters

interface <if-name>: Displays the ability of the specified port to
vlan <vlan-id>: Displays the query port of the specified vlan.

Description

Displays the query port information.

Examples

Show query ports for vlan1.

```
Switch#show ipv6 mld snooping mrouter vlan 1
Bridge VLAN Ports
--------------- ----- -----------------
1 1 ge1/3,
Switch#
```

show ipv6 mld snooping statistics

Command

```
show ipv6 mld snooping statistics [vlan <vlan-id>]
```

Mode

Normal mode / Privilege mode

Parameters

vlan <vlan-id>: Displays the status of the specified vlan.

Description

Displays statistics for MLD protocol packets.

Examples

Display MLD protocol packet statistics for vlan1.

```
Switch#show ipv6 mld snooping statistics vlan 1
```

MLDsnooping debugging commands

debug mld snooping

Command

```
debug mld snooping [all] | [cli] | [events] | [packet] | [timer]
no debug mld snooping [all] | [cli] | [events] | [packet] | [timer]
```

Mode

Privilege mode.

Parameters

all: Turn on all debug switches for mld snooping.
cli: cli command prompt.
events: Turn on the mld snooping time debugging switch.
packet: Turn on the mld snooping packet debugging switch.
timer: Turn on the mld snooping timer debug switch.

Description

The debug igmp snooping command is used to turn on the mld snooping-related debug switch, enabling the user to see the events and messages sent and received related to mld snooping.
The no debug mld snooping command disables the corresponding mld snooping debug switch.

Examples

Turn on the mld snooping message debugging switch.

```
Switch#debug mld snooping packet
Switch#
```

CHAPTER 38

POE commands

POE configuration commands

poemax-power

Command

```
poe max-power <max-power-value>
no poe max-power
```

Mode

Global configuration mode

Parameters

max-power-value: the maximum power value in W, can be set in the range of 20-1000.

Description

The poe max-power command is to set the global maximum output power of the POE power supply.
The no poe max-power command restores the global maximum output power to the default value.

Examples

Set the global maximum output power to 100W

```
Switch# config terminal
Switch(config)# poe max-power 100
#Restore global maximum output power to default value
Switch(config)# no poe max-power
```

poe legacy

Command

```
poe legacy{enable | disable }
```

Mode

Global configuration mode

Parameters

None.

Description

The poe legacy command is to set POE compatibility.

Examples

Set poe compatibility feature

```
Switch# config terminal
Switch(config)# poe legacy
```

poeenable

Command

```
poe enable
no poe enable
```

Mode

Interface configuration mode

Parameters
None.

Description
The poe enable command is to turn on the POE power supply of the interface, which is on by default.
The no poe enable command disables POE power to the interface.

Examples
Shut down power to interface ge1/1

```
Switch# config terminal
Switch(config)# interface ge1/1
Switch(config-ge1/1)# no poe enable
```

poe policy enable

Command

```
poe policy enable
no poe policy enable
```

Mode
Interface configuration mode

Parameters
None.

Description
Turn on or off the interface POE policy, the default interface POE policy is off

Examples
Turn on the POE policy function for interface ge1/1

```
Switch# config terminal
Switch(config)# interface ge1/1
Switch(config-ge1/1)# poe policy enable
```

poepolicy shutdown

Command

```
poe policy shutdown clock <clock-value> week-day <day-value>
no poe policy shutdown clock <clock-value> week-day <day-value>
```

Mode
Interface configuration mode

Parameters
clock-value The time or time range, in 24-hour format.
day-value The day of the week, indicating a certain day or consecutive days

Description
Set or cancel the POE policy entry of the interface, this command can be set multiple times, no POE policy entry is set by default. clock-value is the time or time range, 24-hour system, such as the value of 1 means 1 o'clock (i.e., between 1 o'clock and 2 o'clock), 20-23 means 20 o'clock to 23 o'clock (i.e., between 20 o'clock and 0 o'clock). day-value is the day of the week, indicating a certain day or consecutive days, such as 3 means Wednesday, 1-7 means Monday to Sunday. The POE policy can only take effect if the POE policy of the interface is open.

Examples
Set to turn off POE function on port ge1/1 every Monday from 1:00 to 2:00

```
Switch# config terminal
Switch(config)# interface ge1/1
Switch(config-ge1/1)# poe policy shutdown clock 1 week-day 1
```

poepd-boot-time

Command

```
poe pd-boot-time <time>
no poe pd-boot-time
```

Mode

Interface configuration mode

Parameters

time: the start time of PD, range: 30-600 seconds. Default is 120 seconds.

Description

The poe pd-boot-time command is to set the boot time of PD, the default PD boot time is set to 120 seconds

Examples

```
#Adjust the start-up time of PD for interface ge1/3 to 200 seconds
Switch# config terminal
Switch(config)# interface ge1/3
Switch(config-ge1/3)# poe pd-boot-time 200
```

poepd-timeout-number

Command

```
poe pd-timeout-number< number>
no poe pd-timeout-number
```

Mode

Interface configuration mode

Parameters

number: the number of timeout, range: 2-10 times. Default is 3 times.

Description

The poe pd-timeout-number command is to set the timeout number of querying PD, and the default timeout number of querying PD is 3 times

Examples

```
#Adjust the number of timeouts for PD of interface ge1/3 to 5 times
Switch# config terminal
Switch(config)# interface ge1/3
Switch(config-ge1/3)# poe pd-timeout-number 5
```

poepd-ip-address

Command

```
poe pd-ip-address <ip-address>
no poe pd-ip-address
```

Mode

Interface configuration mode

Parameters

ip-address: IP address of the pd.

Description

The poe pd-ip-address command is to set or clear the IP address of the PD connected to the interface. By default, the IP address of the PD is not configured. If the IP address of the PD is configured, the system will query this IP address regularly, and if the PD does not respond at a given number of times, the PD will be restarted through POE control.

Examples

Set the ip address of PD of interface ge1/3 to 192.168.0.3

```
switch# config terminal
switch(config)# interface ge1/3
switch(config-ge1/3)# poe pd-ip-address 192.168.0.3
```

poe pd-query-interval

Command

```
poe pd-query-interval <interval>
no poe pd-query-interval
```

Mode

Interface configuration mode

Parameters

interval: the interval value, in the range <2-30>.

Description

The poe pd-query-interval command is to set the time interval for querying PD. The default time interval for querying PD is 5 seconds.

Examples

Set the query interval for PD of interface ge1/3 to 5

```
Switch# config terminal
Switch(config)# interface ge1/3
Switch(config-ge1/3)#poe pd-query-interval 5
```

POE view command

show poe

Command

```
show poe
```

Mode

Privilege mode / Normal mode.

Parameters

None.

Description

The show poe command displays the global POE information and POE information of all interfaces.

Examples

Display POE information

```
Switch#show poe
Port Status Operation Type Power(mW) Current(mA) Voltage(V) Class
------ -------- --------- ------- --------- ----------- ---------- -----
ge1/1 Enable Off 802.3at N/A N/A N/A N/A
ge1/2 Enable Off 802.3at N/A N/A N/A N/A
ge1/3 Enable Off 802.3at N/A N/A N/A N/A
ge1/4 Enable Off 802.3at N/A N/A N/A N/A
ge1/5 Enable Off 802.3at N/A N/A N/A N/A
ge1/6 Enable Off 802.3at N/A N/A N/A N/A
ge1/7 Enable Off 802.3at N/A N/A N/A N/A
ge1/8 Enable Off 802.3at N/A N/A N/A N/A
ge1/9 Enable Off 802.3at N/A N/A N/A N/A
ge1/10 Enable Off 802.3at N/A N/A N/A N/A
ge1/11 Enable Off 802.3at N/A N/A N/A N/A
```

```
ge1/12 Enable Off 802.3at N/A N/A N/A N/A
ge1/13 Enable Off 802.3at N/A N/A N/A N/A
ge1/14 Enable Off 802.3at N/A N/A N/A N/A
ge1/15 Enable Off 802.3at N/A N/A N/A N/A
ge1/16 Enable Off 802.3at N/A N/A N/A N/A
ge1/17 Enable Off 802.3at N/A N/A N/A N/A
ge1/18 Enable Off 802.3at N/A N/A N/A N/A
ge1/19 Enable Off 802.3at N/A N/A N/A N/A
ge1/20 Enable Off 802.3at N/A N/A N/A N/A
ge1/21 Enable Off 802.3at N/A N/A N/A N/A
ge1/22 Enable Off 802.3at N/A N/A N/A N/A
ge1/23 Enable Off 802.3at N/A N/A N/A N/A
ge1/24 Enable Off 802.3at N/A N/A N/A N/A
Switch#
```

show poe policy

Command

```
show poe policy <if-name>
```

Mode

Privilege mode / Normal mode.

Parameters

if-name: The specific interface.

Description

The show poe policy command is to display the policy information of poe.

Examples

```
#Show policy information for POE on port ge1/1
Switch#show poe policy ge1/1
```

show poepd-information

Command

```
show poepd-information
```

Mode

Privilege mode / Normal mode.

Parameters

None.

Description

The show poepd-information command is to display information about all configured PDs.

Examples

```
#Display pd information
Switch#show poepd-information
```