PLANET
Networking & Communication

Command Guide

XGS3-24040

24-Port Gigabit with 4 Optional 10G slots

Layer 3 IPv6/IPv4 Managed Stackable Switch

XGS3-42000R

4-Slot Layer 3

IPv6/IPv4 Routing Chassis Switch

Content

Chapter 1 Commands for Basic Switch Configuration

1.1 Commands for Basic Configuration

1.1.1 Authentication line

Command:

authentication line {console | sty | web} login {local | radius | tacos}

No authentication line {console | sty | web} login

Function:

Configure VTY (login with Telnet and SSH), Web and Console, so as to select the priority of the authentication mode for the login user. The no form command restores the default authentication mode.

Default:

No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Command Mode:

Global Mode.

Usage Guide:

The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS or TACCACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives correspond protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The **authentication line console login** command is exclusive with the **login** command. The **authentication line console login** command configures the switch to use the Console login method. And the **login** command makes the Console login to use the passwords configured by the **password** command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

Example:

To configure the Telnet and ssh login method to use RADIUS authentication method.

```
Switch(config)# authentication line vty login local radius
```

Relative Command:

aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.1.2 boot img

Command:

boot img <*img-file-url*> { **primary | backup** }

Function:

Configure the first and second img files used in the next boot of the main control boardcard.

Parameters: .

primary means to configure the first IMG file, backup means to configure the second IMG file, <img-file-url> is the full path of the booting IMG file, the format of which is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.
2. The suffix of all file names should be .img.
3. The length of the full file path should be no longer than 128 characters, while the file name no longer than 80 characters.

Command Mode:

Admin Mode.

Default:

The factory original configuration only specifies the first booting IMG file, the nos.img file in the FLASH, without the second one.

Example:

1. Set flash:/nos.img as the second booting IMG file used in the next booting of the system.

```
Switch#boot img flash:/nos.img backup
```

2. Set flash:/5.4.128.0_nos.img as the first booting IMG file used in the next booting of the system.

```
Switch#boot img flash:/5.4.128.0_nos.img primary
```

1.1.3 boot startup-config

Command:

boot startup-config { NULL | <*file-url*> }

Function:

Configure the CGF file used in the next booting of the main control boardcard.

Parameters:

The NULL keyword means to use the factory original configuration as the next booting configuration. Setting the he CGF file used in the next booting as NULL equals to implementing “set default” and “write”. ***<file-url>*** is the full path of CGF file used in the next booting.

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.
2. The suffix of all file names should be .cfg.
3. The length of the full file path should be no longer than 128 characters, while the file name no longer than 80 characters.

Command Mode:

Admin Mode.

Default Settings:

None.

Example:

1. Set flash:/ startup.cfg as the booting CFG file used in the next booting of the system.

```
Switch# boot startup-configflash:/ startup.cfg
```

2. Set flash:/ test-trunk.cfg as the booting CFG file used in the next booting of the system.

```
Switch#boot startup-config flash:/ test-trunk.cfg
```

1.1.4 clock set

Command:

clock set *<HH:MM:SS> <YYYY.MM.DD>*

Function:

Set system date and time.

Parameter:

<HH:MM:SS>is the current time, and the valid scope for ***HH*** is 0 to 23, ***MM*** and ***SS*** 0 to 59; ***<YYYY.MM.DD>*** is the current year, month and date, and the valid scope for ***YYYY*** is 1970~2038, ***MON*** meaning month, and ***DD*** between 1 to 31.

Command mode:

Admin Mode.

Default:

upon first time start-up, it is defaulted to 2001.1.1 0: 0: 0.

Usage guide:

The switch can not continue timing with power off, hence the current date and time must be first set at environments where exact time is required.

Example:

To set the switch current date and time to 2002.8.1 23: 0: 0:

```
Switch#clock set 23:0:0 2002.8.1
```

1.1.5 config

Command:

config [terminal]

Function:

Enter Global Mode from Admin Mode.

Parameter:

[terminal] indicates terminal configuration.

Command mode:

Admin Mode

Example:

```
Switch#config
```

1.1.6 debug ssh-server

Command:

debug ssh-server

no debug ssh-server

Function:

Display SSH server debugging information; the "**no debug ssh-server**" command stops displaying SSH server debugging information.

Default:

This function is disabled by default.

Command mode:

Admin Mode.

Example:

```
Switch#debug ssh-server
```

1.1.7 enable

Command:

enable

disable

Function:

Enter Admin Mode from User Mode.

Command mode:

User Mode/ Admin Mode.

Usage Guide:

To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. Set the Admin user password under Global Mode with "**enable password**" command.

Example:

```
Switch>enable
```

```
Switch#
```

1.1.8 enable password

Command:

enable password [8] <password>

no enable password

Function:

Configure the password used for enter Admin Mode from the User Mode,

The "**no enable password**" command deletes this password.

Parameter:

password is the configured code. Encryption will be performed by entering 8.

Command mode:

Global Mode

Default:

This password is empty by system default

Usage Guide:

Configure this password to prevent unauthorized entering Admin Mode. It is recommended to set the password at the initial switch configuration. Also, it is recommended to exit Admin Mode with "**exit**" command when the administrator needs to leave the terminal for a long time.

Example:

Set the Admin user password to "admin".

```
Switch(config)#enable password 8 admin
```

1.1.9 end

Command:

end

Function:

Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.

Command mode:

Except User Mode/ Admin Mode

Example:

Quit VLAN mode and return to Admin mode.

```
Switch(config-vlan1)#end
Switch#
```

1.1.10 exec-timeout

Command:

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

no exec-timeout

Function:

Configure the timeout of exiting admin mode. The "**no exec-timeout**" command restores the default value.

Parameters:

<minute> is the time value shown in minute and ranges between 0~35791.<seconds> is the time value shown in seconds and ranges between 0~2147483.

Command mode:

Global mode

Default:

Default timeout is 10 minutes.

Usage guide:

To secure the switch, as well to prevent malicious actions from unauthorized user, the time will be count from the last configuration the admin had made, and the system will exit the admin mode at due time. It is required to enter admin code and password to enter the admin mode again. The timeout timer will be disabled when the timeout is set to 0.

Example:

Set the admin mode timeout value to 6 minutes

```
Switch(config)#exec-timeout 6
```

Set the admin mode timeout value to 5 minutes, 30 seconds

```
Switch(config)#exec-timeout 5 30
```

1.1.11 exit

Command:

exit

Function:

Quit current mode and return to it's previous mode.

Command mode:

All Modes

Usage Guide:

This command is to quit current mode and return to it's previous mode.

Example:

Quit global mode to it's previous mode

```
Switch#exit
```

```
Switch#
```

1.1.12 help

Command:

help

Function:

Output brief description of the command interpreter help system.

Command mode:

All configuration modes.

Usage Guide:

An instant online help provided by the switch. Help command displays information about the whole help system,

including complete help and partial help. The user can type in ? any time to get online help.

Example:

```
switch(config)#help
```

PLANETOS CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:

1. Full help is available when you are ready to enter acommand argument (e.g. 'show ?')
   and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

1.1.13 hostname

Command:

hostname <*hostname*>

no hostname

Function:

Set the prompt in the switch command line interface. The no operation cancels the configuration.

Parameter:

<hostname> is the string for the prompt, up to 30 characters are allowed.

Command mode:

Global Mode

Default:

The default prompt is relatived with the switch.

Usage Guide:

With this command, the user can set the CLI prompt of the switch according to their own requirements.

Example:

Set the prompt to “Test”.

```
Switch(config)#hostname Test
```

```
Test(config)#
```

1.1.14 ip host

Command:

ip host <*hostname*> <*ip_addr*>

no ip host {<*hostname*>|all}

Function:

Set the mapping relationship between the host and IP address; the “no ip host” parameter of this command will

delete the mapping.

Parameter:

<hostname> is the host name, up to 15 characters are allowed; ***<ip_addr>*** is the corresponding IP address for the host name, takes a dot decimal format; **all** is all of the host name.

Command mode:

Global Mode

Usage Guide:

Set the association between host and IP address, which can be used in commands like "**ping *<host>***".

Example:

Set IP address of a host with the hostname of "beijing" to 200.121.1.1.

```
Switch(config)#ip host beijing 200.121.1.1
```

Command related:

telnet, ping, traceroute

1.1.15 ipv6 host

Command:

ipv6 host *<hostname>* *<ipv6_addr>*

no ipv6 host {*<hostname>*|all}

Function:

Configure the mapping relationship between the IPv6 address and the host; the "**no ipv6 host *<hostname>***" command deletes this mapping relationship.

Parameter:

<hostname> is the name of the host, containing max 15 characters;***<ipv6_addr>*** is the IPv6 address corresponding to the host name.<all> is all the host address.

Command Mode:

Global Mode

Usage Guide:

Configure a fixed corresponding relationship between the host and the IPv6 address, applicable in commands such as "**traceroute6 <host>**", etc.

Example:

Set the IPv6 address of the host named beijing to 2001:1:2:3::1

```
Switch(config)#ipv6 host beijing 2001:1:2:3::1
```

Command related:

ping6,traceroute6

1.1.16 ip http server

Command:

ip http server

no ip http server

Function:

Enable Web configuration; the "**no ip http server**" command disables Web configuration

Command mode:

Global mode

Usage guide:

Web configuation is for supplying a interface configured with HTTP for the user, which is straight and visual, esay to understand.

Example:

Enable Web Server function and enable Web configurations.

```
Switch(config)#ip http server
```

1.1.17 language

Command:

language {chinese | english}

Function:

Set the language for displaying the help information.

Parameter:

chinese for Chinese display; **english** for English display.

Command mode:

Admin and Config Mode.

Default:

The default setting is English display.

Usage Guide:

Switch provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information display will revert to English.

1.1.18 login

Command:

login

no login

Function:

login enable password authentication, no login command cancels the login configuration.

Command mode:

Global mode

Default:

No login by default

Usage guide:

By using this command, users have to enter the password set by password command to enter normal user mode with console; no login cancels this restriction.

Example:

Enable password

```
Switch(config)#login
```

1.1.19 password

Command:

password [8] <*password*>

no password

Function:

Configure the password used for enter normal user mode on the console. The "**no password**" command deletes this password.

Parameter:

password is the configured code. Encryption will be performed by entering 8.

Command mode:

Global mode

Default:

This password is empty by system default

Usage guide:

When both this password and login command are configured, users have to enter the password set by password command to enter normal user mode on console.

Example:

```
Switch(config)#password 8 test
Switch(config)#login
```

1.1.20 reload

Command:

reload

Function:

Warm reset the switch.

Command mode:

Admin Mode.

Usage Guide:

The user can use this command to restart the switch without power off.

1.1.21 service password-encryption

Command:

service password-encryption

no service password-encryption

Function:

Encrypt system password. The "**no service password-encryption**" command cancels the encryption.

Command mode:

Global Mode

Default:

No service password-encryption by system default

Usage guide:

The current unencrypted passwords as well as the coming passwords configured by password, enable password and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.

Example:

Encrypt system passwords

```
Switch(config)#service password-encryption
```

```

```

1.1.22 service terminal-length

Command:

service terminal-length <0-512>

no service terminal-length

Function:

Configure the columns of characters displayed in each screen on terminal (vty). The "**no service terminal-length**" command cancels the screen shifting operation.

Parameter:

Columns of characters displayed on each screen of vty, ranging between 0-512.

Command mode:

Global Mode

Usage guide:

Configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telent.ssh client and the Console will be following this configuration.

Example:

Set the number of vty threads to 20.

```
Switch(config)#service terminal-length 20
```

1.1.23 sysContact

Command:

sysContact <LINE>

no sysContact

Function:

Set the factory contact mode, the "**no sysContact**" command reset the switch to factory settings.

Parameter:

<LINE> is the prompt character string, range from 0 to 255 characters.

Command mode:

Global Mode

Default:

The factory settings.

Usage guide:

The user can set the factory contact mode bases the fact instance.

Example:

Set the factory contact mode to test.

```
Switch(config)#sysContact test
```

1.1.24 sysLocation

Command:

sysLocation <LINE>

no sysLocation

Function:

Set the factory address, the "**no sysLocation**" command reset the switch to factory settings.

Parameter:

<LINE> is the prompt character string, range from 0 to 255 characters.

Command mode:

Global Mode

Default:

The factory settings.

Usage guide:

The user can set the factory address bases the fact instance.

Example:

Set the factory address to test.

```
Switch(config)#sysLocation test
```

1.1.25 set default

Command:

set default

Function:

Reset the switch to factory settings.

Command mode:

Admin Mode.

Usage Guide:

Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.

Note:

After the command, "**write**" command must be executed to save the operation. The switch will reset to factory settings after restart.

Example:

```
Switch#set default
```

Are you sure? [Y/N] = y

```
Switch#write
Switch#reload
```

1.1.26 setup

Command:

setup

Function:

Enter the Setup Mode of the switch.

Command mode:

Admin Mode.

Usage Guide:

Switch provides a Setup Mode, in which the user can configure IP addresses, etc.

1.1.27 show clock

Command:

show clock

Function:

Display the current system clock.

Command mode:

Admin and Configuration Mode.

Usage Guide:

If the system clock is inaccurate, user can adjust the time by examining the system date and clock.

Example:

```
Switch#show clock
Current time is TUE AUG 22 11：00：01 2002
```

Command related:

clock set

1.1.28 show temperature

Command:

show temperature

Function:

Display the current temputerature of the switch CPU.

Command mode:

All mode.

Usage Guide:

This command is used to monitor the temperature of the switch CPU.

Example:

Display the current temperature of the switch CPU.

```
Switch(Config)#show temperature
Temperature: 47.0625 ℃
```

1.1.29 show tech-support

Command:

show tech-support

Function:

Display the operational information and the task status of the switch. The technique specialist use this command to diagnose whether the switch operate normally.

Command mode:

Admin and Configuration Mode.

Usage Guide:

This command is used to collect the relative information when the switch operation is malfunctioned.

Example:

```
Switch#show tech-support
```

1.1.30 show version

Command:

show version

Function:

Display the version information of the switch.

Command mode:

Admin and Configuration Mode.

Usage Guide:

this command is used to show the version information of the switch, including the hardware version and the software version information.

Example:

```
Switch#show version.
```

1.1.31 username

Command:

username <*username*> [privilege <*privilege*>] [password <*0|7*> <*password*>]

no username <*username*>

Function:

Configure local login username and password along with its privilege level.

Parameter:

<username> is the name of the user. ***<privilege>*** is the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default. ***<password>*** is the password for the user. If input option 7 on password setting, the password is encrypted; if input option 0, the password is not processed.

Command Mode:

Global Mode.

Usage Guide:

There are two available choices for the preferences of the registered commands in the switch. They are 1 and 15. Preference of 1 is for the commands of the normal user configuration mode. Preference of 15 is for the commands registered in modes other than the normal user configuration modes. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.

Notice:

The user can log in user and priority after the command configures, before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode. If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.

Example:

Configure an administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.

Above all the configurations, only the admin user is able to login the switch in privileged mode through Telnet or

Console login method, user1 and user2 can only login the switch in normal user mode through the telnet and console login method. For HTTP login method, only the admin user can pass the authentication configuration, user1 and user2 will be denied.

Switch(config)#username admin privilege 15 password 0 admin
Switch(config)# username user1 privilege 1 password 7 user1
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local

1.1.32 web language

Command:

web language {chinese | english}

Function:

Set the language for displaying the HTTP Server information.

Parameter:

chinese for Chinese display; **english** for English display.

Command mode:

Admin Mode

Default:

The default setting is English display.

Usage Guide:

The user can select the language according to their preference.

1.1.33 write

Command:

write

Function:

Save the currently configured parameters to the Flash memory.

Command mode:

Admin Mode.

Usage Guide:

After a set of configuration with desired functions, the setting should be saved to the Flash memory, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the **copy running-config startup-config** command.

1.2 Commands for Telnet

1.2.1 authentication ip access-class

Command:

authentication ip access-class {<num-std>|<name>}

no authentication ip access-class

Function:

Binding standard IP ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

Parameters:

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99; <name> is the access-class name for standard ACL, the character string length is ranging between 1-32.

Default:

The binding ACL to Telnet/SSH/Web function is closed by default.

Command Mode:

Global Mode.

Example:

Binding standard IP ACL protocol to access-class 1.

```
Switch(config)#authentication ip access-class 1
```

1.2.2 authentication ipv6 access-class

Command:

authentication ipv6 access-class {<num-std>|<name>}

no authentication ipv6 access-class

Function:

Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

Parameters:

<num-std> is the access-class number for standard numeric ACL, ranging between 500-599; <name> is the access-class name for standard ACL, the character string length is ranging between 1-32.

Default:

The binding ACL to Telnet/SSH/Web function is closed by default.

Command Mode:

Global Mode.

Example:

Binding standard IP ACL protocol to access-class 500.

```
Switch(config)#authentication ipv6 access-class 500
```

1.2.3 authentication line login

Command:

authentication line {console | vty | web} login {local | radius | tacacs}

no authentication line {console | vty | web} login

Function:

Configure VTY (login with Telnet and SSH), Web and Console, so as to select the priority of the authentication mode for the login user. The no form command restores the default authentication mode.

Default:

No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Command Mode:

Global Mode.

Usage Guide:

The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS or TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives correspond protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The **authentication line console login** command is exclusive with the "**login**" command. The **authentication line console login** command configures the switch to use the Console login method. And the **login** command makes the Console login to use the passwords configured by the **password** command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

Example:

Configure the remote login authentication mode to radius.

```
Switch(config)#authentication login radius
```

Relative Command:

aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.2.4 authentication securityip

Command:

authentication securityip <*ip*

no authentication securityip <*ip-addr*>

Function:

To configure the trusted IP address for Telnet and HTTP login method. The no form of this command will remove the trusted IP address configuration.

Parameters:

<ip-addr> is the trusted IP address of the client in dotted decimal format which can login the switch.

Default:

No trusted IP address is configured by default.

Command Mode:

Global Mode.

Usage Guide:

IP address of the client which can login the switch is not restricted before the trusted IP address is not configured. After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch.

Example:

To configure 192.168.1.21 as the trusted IP address.

```
Switch(config)# authentication securityip 192.168.1.21
```

1.2.5 authentication securityipv6

Command:

authentication securityipv6 <*ipv6-addr*>

no authentication securityipv6 <*ipv6-addr*>

Function:

To configure the trusted IPv6 address for Telnet and HTTP login method. The no form of this command will remove the specified configuration.

Parameters:

<ipv6-addr> is the trusted IPv6 address which can login the switch.

Default:

No trusted IPv6 addresses are configured by default.

Command Mode:

Global Mode.

Usage Guide:

IPv6 address of the client which can login the switch is not restricted before the trusted IPv6 address is not configured. After the trusted IPv6 address is configured, only clients with trusted IPv6 addresses are able to login the switch. Up to 32 trusted IPv6 addresses can be configured in the switch.

Example:

Configure the secure IPv6 address is 2001:da8:123:1::1.

```
Switch(config)# authentication securityipv6 2001:da8:123:1::1
```

1.2.6 terminal length

Command:

terminal length <0-512>

terminal no length

Function:

Set columns of characters displayed in each screen on terminal; the "**terminal no length**" cancels the screen switching operation and display content once in all.

Parameter:

Columns of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display).

Command mode:

Admin Mode.

Default:

Default columns is 25.

Usage guide:

Set columns of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen. 25 columns by default.

Example:

Configure treads in each display to 20.

```
Switch#terminal length 20
```

1.2.7 terminal monitor

Command:

terminal monitor

terminal no monitor

Function:

Copy debugging messages to current display terminal; the "**terminal no monitor**" command restores to the default value.

Command mode:

Admin Mode.

Usage guide:

Configures whether the current debugging messages is displayed on this terminal. If this command is configured on telnet or SSH clients, debug messages will be sent to that client. The debug message is displayed on console by default.

Example:

```
Switch#terminal monitor
```

1.2.8 telnet

Command:

telnet {<*ip-addr*> | <*ipv6-addr*> | host <*hostname*>} [<*port*>]

Function:

Log on the remote host by Telnet

Parameter:

<ip-addr> is the IP address of the remote host, shown in dotted decimal notation; **<ipv6-addr>** is the IPv6 address of the remote host; ***<hostname>*** is the name of the remote host, containing max 30 characters; ***<port>*** is the port number, ranging between 0~65535.

Command Mode:

Admin Mode.

Usage Guide:

This command is used when the switch is applied as Telnet client, for logging on remote host to configure. When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey "CTRL+ \". To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.

Example:

The switch Telnets to a remote host whose IP address is 20.1.1.1.

```
Switch#telnet 20.1.1.1 23
Connecting Host 20.1.1.1 Port 23
Service port is 23
Connected to 20.1.1.1
login:123
password:***
XGS3>
```

1.2.9 telnet server enable

Command:

telnet server enable

no telnet server enable

Function:

Enable the Telnet server function in the switch: the “no telnet server enable” command disables the Telnet function in the switch.

Default:

Telnet server function is enabled by default.

Command mode:

Global Mode

Usage Guide:

This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch.

Example:

Disable the Telnet server function in the switch.

```
Switch(config)#no telnet server enable
```

1.2.10 telnet-server max-connection

Command:

telnet-server max-connection {<max-connection-number> | default}

Function:

Configure the max connection number supported by the Telnet service of the switch.

Parameters:

<max-connection-number>: the max connection number supported by the Telnet service, ranging from 5 to 16. The default option will restore the default configuration.

Default:

The system default value of the max connection number is 5.

Command Mode:

Global Mode

Usage Guide:

None.

Example:

Set the max connection number supported by the Telnet service as 10.

```
Switch(config)#telnet-server max-connection 10
```

1.2.11 ssh-server authentication-retries

Command:

ssh-server authentication-retries <authentication-retries>

no ssh-server authentication-retries

Function:

Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.

Parameter:

authentication-retries > is the number of times for retrying authentication; valid range is 1 to 10.

Command mode:

Global Mode

Default:

The number of times for retrying SSH authentication is 3 by default.

Example:

Set the number of times for retrying SSH authentication to 5.

```
Switch(config)#ssh-server authentication-retries 5
```

1.2.12 ssh-server enable

Command:

ssh-server enable

no ssh-server enable

Function:

Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.

Command mode:

Global Mode

Default:

SSH function is disabled by default.

Usage Guide:

In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch.

Example:

Enable SSH function on the switch.

```
Switch(config)#ssh-server enable
```

1.2.13 ssh-server host-key create rsa

Command:

ssh-server host-key create rsa [modulus < modulus >]

Function:

Generate new RSA host key.

Parameter:

modulus is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.

Command mode:

Global Mode

Default:

The system uses the key generated when the ssh-server is started at the first time.

Usage Guide:

This command is used to generate the new host key. When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and “write” command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.

Example:

Generate new host key.

```
Switch(config)#ssh-server host-key create rsa
```

1.2.14 ssh-server max-connection

Command:

ssh-server max-connection {<max-connection-number>|default}

Function:

Configure the max connection number supported by the SSH service of the switch.

Parameters:

<max-connection-number>: the max connection number supported by the SSH service, ranging from 5 to 16. The default option will restore the default configuration.

Default:

The system default value of the max connection number is 5.

Command Mode:

Global Mode

Usage Guide:

None.

Example:

Set the max connection number supported by the SSH service as 10.

```
Switch(config)#ssh-server max-connection 10
```

1.2.15 ssh-server timeout

Command:

ssh-server timeout <timeout>

no ssh-server timeout

Function:

Configure timeout value for SSH authentication; the “**no ssh-server timeout**” command restores the default timeout value for SSH authentication.

Parameter:

<timeout> is timeout value; valid range is 10 to 600 seconds.

Command mode:

Global Mode

Default:

SSH authentication timeout is 180 seconds by default.

Example:

Set SSH authentication timeout to 240 seconds.

```
Switch(config)#ssh-server timeout 240
```

1.2.16 ssh-user

Command:

ssh-user <*username*> password {0 | 7} <*password*>

no ssh-user <*username*>

Function:

Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.

Parameter:

<username> is SSH client username. It can't exceed 16 characters; ***<password>*** is SSH client password. It can't exceed 32 characters; **0 | 7** stand for unencrypted password and encrypted password.

Command mode:

Global Mode

Default:

There are no SSH username and password by default.

Usage Guide:

This command is used to configure the authorized SSH client. Any unauthorized SSH clients can't log on and configure the switch.

Example:

Set a SSH client which has "switch" as username and "switch" as password.

```
Switch(config)#ssh-user switch password 0 switch
```

1.2.17 show ssh-server

Command:

show ssh-server

Function:

Display SSH state and users which log on currently.

Command mode:

Admin Mode.

Example:

```
Switch#show ssh-server
ssh server is enabled
ssh-server timeout 180s
ssh-server authentication-retries 3
ssh-server max-connection number 6
ssh-server login user number 2
```

1.2.18 show ssh-user

Command:

show ssh-user

Function:

Display the configured SSH usernames.

Command Mode:

Admin Mode.

Example:

```
Switch#show ssh-user
test
```

Relative Command:

ssh-user, ssh-server enable, no ssh-server enable

1.2.19 show telnet login

Command:

show telnet login

Function:

Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

Check the Telnet client messages connected through Telnet with the switch.

Example:

```
Switch#show telnet login
Authenticate login by local
Login user:
aa
```

1.3 Commands for Configuring Switch IP

1.3.1 interface vlan

Command:

interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function:

Enter the VLAN interface configuration mode; the no operation of this command will delete the existing VLAN interface.

Parameters:

<vlan-id> is the VLAN ID of an existing VLAN, ranging from 1 to 4094.

Command Mode:

Global Configuration Mode.

Usage Guide:

Users should first make sure the existence of a VLAN before configuring it. User "**exit**" command to quit the VLAN interface configuration mode back to the global configuration mode.

Example:

Enter the VLAN interface configuration mode of VLAN1.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#
```

1.3.2 interface ethernet 0

This command is not supported by the switch.

1.3.3 ip address

Command:

ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function:

Set the IP address and mask for the specified VLAN interface; the "**no ip address <*ip address*> <*mask*> [secondary]**" command deletes the specified IP address setting.

Parameter:

<ip-address> is the IP address in dot decimal format; ***<mask>*** is the subnet mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Default:

No IP address is configured upon switch shipment.

Command mode:

VLAN Interface Mode

Usage Guide:

A VLAN interface must be created first before the user can assign an IP address to the switch.

Example:

Set 10.1.128.1/24 as the IP address of VLAN1 interface.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

Relative Command:

ip bootp-client enable, ip dhcp-client enable

1.3.4 ipv6 address

Command:

ipv6 address <*ipv6address* | *prefix-length*> [eui-64]

no ipv6 address <*ipv6address* | *prefix-length*> [eui-64]

Function:

Configure aggregatable global unicast address, site-local address and link-local address for the interface.

Parameters:

<ipv6address> is the prefix of an IPV6 address; ***<prefix-length>***is the length of the prefix of an IPV6 address, ranging from 3 to 128; eui-64 means that the eui64 interface id of the interface will automatically create an IPV6 address.

Command Mode:

Interface Configuration Mode.

Default

None.

Usage Guide:

The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage. Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff ::,with a length no shorter than 3. And the prefix length of a site-local address or a link-local address should not be shorter than 10.

Examples:

Configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64.

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

1.3.5 ip bootp-client enable

Command:

ip bootp-client enable

no ip bootp-client enable

Function:

Enable the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP Client function and releases the IP address obtained in BootP.

Default:

BootP client function is disabled by default.

Command mode:

VLAN Interface Mode

Usage Guide:

Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed. Note: To obtain IP address via BootP, a DHCP server or a BootP server is required in the network.

Example:

Get IP address through BootP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip bootp-client enable
Switch (Config-if-Vlan1)#exit
Switch(config)#
```

Relative command:

ip address, ip dhcp-client enable

1.3.6 ip dhcp-client enable

Command:

ip dhcp-client enable

no ip dhcp-client enable

Function:

Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp-client enable**" command disables the DHCP client function and releases the IP address obtained in DHCP. Note: To obtain IP address via DHCP, a DHCP server is required in the network.

Default:

the DHCP client function is disabled by default.

Command mode:

VLAN Interface Mode

Usage Guide:

Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.

Example:

Getting an IP address through DHCP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

1.4 Commands for SNMP

1.4.1 debug snmp mib

Command:

debug snmp mib

no debug snmp mib

Function:

Enable the SNMP mib debugging; the "**no debug snmp mib**" command disables the debugging.

Command Mode:

Admin Mode.

Usage Guide:

When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

```
Switch#debug snmp mib
```

1.4.2 debug snmp kernel

Command:

debug snmp kernel

no debug snmp kernel

Function:

Enable the SNMP kernel debugging; the "**no debug snmp kernel**" command disables the debugging function.

Command Mode:

Admin Mode.

Usage Guide:

When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

```
Switch#debug snmp kernel
```

1.4.3 rmon enable

Command:

rmon enable

no rmon enable

Function:

Enable RMON; the "**no rmon enable**" command disables RMON.

Command mode:

Global Mode

Default:

RMON is disabled by default.

Example:

Enable RMON.

```
Switch(config)#rmon enable
```

Disable RMON.

```
Switch(config)#no rmon enable
```

1.4.4 show snmp

Command:

show snmp

Function:

Display all SNMP counter information.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp
    0 SNMP packets input
            0 Bad SNMP version errors
            0 Unknown community name
            0 Illegal operation for community name supplied
           0 Encoding errors
           0 Number of requested variables
           0 Number of altered variables
           0 Get-request PDUs
           0 Get-next PDUs
           0 Set-request PDUs
  0 SNMP packets output
```

```
0 Too big errors (Max packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs
```

Displayed information Explanation
snmp packets input Total number of SNMP packet inputs.
bad snmp version errors Number of version information error packets.
unknown community name Number of community name error packets.
illegal operation for community name supplied Number of permission for community name error packets.
encoding errors Number of encoding error packets.
number of requested variable Number of variables requested by NMS.
number of altered variables Number of variables set by NMS.
get-request PDUs Number of packets received by “get” requests.
get-next PDUs Number of packets received by “getnext” requests.
set-request PDUs Number of packets received by “set” requests.
snmp packets output Total number of SNMP packet outputs.

too big errors Number of “Too_ big” error SNMP packets.
maximum packet size Maximum length of SNMP packets.
no such name errors Number of packets requesting for non-existent MIB objects.
bad values errors Number of “Bad_values” error SNMP packets.
general errors Number of “General_errors” error SNMP packets.
response PDUs Number of response packets sent.
trap PDUs Number of Trap packets sent.

1.4.5 show snmp engineid

Command:

show snmp engineid

Function:

Display the engine ID commands.

Command Mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp engineid
      SNMP engineID:3138633303f1276c          Engine Boots is:1
```

Displayed Information Explanation
SNMP engineID Engine number
Engine Boots Engine boot counts

1.4.6 show snmp group

Command:

show snmp group

Function:

Display the group information commands.

Command Mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp group
    Group Name:initial              Security Level:noAuthnoPriv
    Read View:one
    Write View:<no writeview specified>
    Notify View:one
```

Displayed Information Explanation
Group Name Group name
Security level Security level
Read View Read view name
Write View Write view name
Notify View Notify view name
<no writeview specified> No view name specified by the user

1.4.7 show snmp mib

Command:

show snmp mib

Function:

Display all MIB supported by the switch.

Command Mode:

Admin and Configuration Mode.

1.4.8 show snmp status

Command:

show snmp status

Function:

Display SNMP configuration information.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp status
    Trap enable
    RMON enable
    Community Information:
    V1/V2c Trap Host Information:
    V3 Trap Host Information:
    Security IP Information:
```

Displayed information Description
Community string Community string
Community access Community access permission
Trap-rec-address IP address which is used to receive Trap.
Trap enable Enable or disable to send Trap.
SecurityIP IP address of the NMS which is allowed to access Agent

1.4.9 show snmp user

Command:

show snmp user

Function:

Display the user information commands.

Command Mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp user
    User name: initialsha
    Engine ID: 1234567890
    Auth Protocol:MD5       Priv Protocol:DES-CBC
    Row status:active
```

Displayed Information Explanation
User name User name
Engine ID Engine ID
Priv Protocol Employed encryption algorithm
Auth Protocol Employed identification algorithm
Row status User state

1.4.10 show snmp view

Command:

show snmp view

Function:

Display the view information commands.

Command Mode:

Admin and Configuration Mode.

Example:

```
Switch#show snmp view
```

```
View Name:readview          1.          -Included      active
                1.3.        Excluded    active
```

Displayed Information Explanation
View Name View name
1.and1.3. OID number
Included The view includes sub trees rooted by this OID
Excluded The view does not include sub trees rooted by this OID
active State

1.4.11 snmp-server community

Command:

snmp-server community {ro | rw} <*string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}] [read <*read-view-name*>] [write <*write-view-name*>]

no snmp-server community <*string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]

Function:

Configure the community string for the switch; the "**no snmp-server community <*string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*> |<*ipv6-name*>}]** "command deletes the configured community string.

Parameter:

<string> is the community string set;

ro | rw is the specified access mode to MIB, **ro** for read-only and **rw** for read-write.

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99;

<name> is the access-class name for standard ACL, the character string length is ranging between 1-32;

<ipv6-num-std> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<name> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.

<read-view-name> is the name of readable view which includes 1-32 characters.

<write-view-name> is the name of writable view which includes 1-32 characters.

Command mode:

Global Mode

Usage Guide:

The switch supports up to 4 community strings. It can realize the access-control for specifically community view by binding the community name to specifically readable view or writable view.

Example:

Add a community string named “private” with read-write permission.

```
Switch(config)#snmp-server community private rw
```

Add a community string named “public” with read-only permission.

```
Switch(config)#snmp-server community public ro
```

Modify the read-write community string named “private” to read-only.

```
Switch(config)#snmp-server community private ro
```

Delete community string “private”.

```
Switch(config)#no snmp-server community private
```

Bind the read-only community string “public” to readable view “pviewr”.

```
Switch(config)#snmp-server community ro public read pviewr
```

Bind the read-write community string “private” to readable view “pviewr” and writable view “pvieww”.

```
Switch(config)#snmp-server community rw private read pviewr write pvieww
```

1.4.12 snmp-server enable

Command:

snmp-server enable

no snmp-server enable

Function:

Enable the SNMP proxy server function on the switch. The “**no snmp-server enable**” command disables the SNMP proxy server function

Command mode:

Global mode

Default:

SNMP proxy server function is disabled by system default.

Usage guide:

To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command.

Example:

Enable the SNMP proxy server function on the switch.

```
Switch(config)#snmp-server enable
```

1.4.13 snmp-server enable traps

Command:

snmp-server enable traps

no snmp-server enable traps

Function:

Enable the switch to send Trap message; the "**no snmp-server enable traps**" command disables the switch to send Trap message.

Command mode:

Global Mode

Default:

Trap message is disabled by default.

Usage Guide:

When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

Example:

Enable to send Trap messages.

```
Switch(config)#snmp-server enable traps
```

Disable to send Trap messages.

```
Switch(config)#no snmp-server enable traps
```

1.4.14 snmp-server engineid

Command:

snmp-server engineid <*engine-string*>

no snmp-server engineid

Function:

Configure the engine ID; the "no" form of this command restores to the default engine ID.

Command Mode:

Global mode

Parameter:

<*engine-string*> is the engine ID shown in 1-32 digit hex characters.

Default:

Default value is the company ID plus local MAC address.

Usage Guide:

None

Example:

Set current engine ID to A66688999F

```
Switch(config)#snmp-server engineid A66688999F
```

Restore the default engine ID

```
Switch(config)#no snmp-server engineid
```

1.4.15 snmp-server group

Command:

snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]

no snmp-server group <*group-string*> {NoauthNopriv | AuthNopriv | AuthPriv} [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]

Function:

This command is used to configure a new group; the “no” form of this command deletes this group.

Command Mode:

Global Mode

Parameter:

<group-string> group name which includes 1-32 characters

NoauthNopriv Applies the non recognizing and non encrypting safety level

AuthNopriv Applies the recognizing but non encrypting safety level

AuthPriv Applies the recognizing and encrypting safety level

read-string Name of readable view which includes 1-32 characters

write-string Name of writable view which includes 1-32 characters

notify-string Name of trappable view which includes 1-32 characters

<*num-std*> is the access-class number for standard numeric ACL, ranging between 1-99;

<*name*> is the access-class name for standard ACL, the character string length is ranging between 1-32;

<*ipv6-num-std*> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<*name*> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.

Usage Guide:

There is a default view “v1defaultviewname” in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled.

Example:

Create a group CompanyGroup, with the safety level of recognizing andencrypting, the read viewname isreadview, and the writing is disabled.

```
Switch (config)#snmp-server group CompanyGroup AuthPriv read readview
```

deletet group

```
Switch (config)#no snmp-server group CompanyGroup AuthPriv
```

1.4.16 snmp-server host

Command:

snmp-server host { <*host-ipv4-address*> | <*host-ipv6-address*> } {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <*user-string*>

no snmp-server host { <*host-ipv4-address*> | <*host-ipv6-address*> } {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <*user-string*>

Function:

As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for

receiving the network manage station IPv4 or IPv6 address and the Trap user name and safety level; the “no” form of this command cancels this IPv4 or IPv6 address.

Command Mode:

Global Mode.

Parameter:

<host-ipv4-addr>* | *<host-ipv6-addr> is the IP address of the NMS managing station which receives Trap message.

v1 | v2c | v3 is the version number when sending the trap.

NoauthNopriv | AuthNopriv | AuthPriv is the safety level v3 trap is applied, which may be non encrypted and non authentication, non encrypted and authentication, encrypted and authentication.

<user-*string*> is the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3.

Usage Guide:

The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but configure the version number as v1 and v2c of the IPv4 and IPv6 address are less than 8 in all.

Example:

Configure an IP address to receive Trap

```
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
```

Delete a Trap receiving IPv6 address

```
Switch(config)#no snmp-server host 2001:1:2:3::1 v1 usertrap
```

1.4.17 snmp-server securityip

Command:

snmp-server securityip {<ipv4-address> | *<ipv6-address>*}

no snmp-server securityip {<ipv4-address> | *<ipv6-address>*}

Function:

Configure to permit to access security IPv4 or IPv6 address of the switch NMS administration station; the no command deletes configured security IPv4 or IPv6 address.

Command Mode:

Global Mode.

Parameter:

<ipv4-address> is NMS security IPv4 address, point separated decimal format.

<ipv6-address> is NMS security IPv6 address, colon separated hex format.

Usage Guide:

It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP packet could be processed by switch, the command only applies to SNMP. Allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but the IP addresses are less than 6 in all.

Example:

Configure security IP address of NMS administration station

```
Switch(config)#snmp-server securityip 1.1.1.5
```

Delete security IPv6 address

```
Switch(config)#no snmp-server securityip 2001::1
```

1.4.18 snmp-server securityip

Command:

snmp-server securityip {enable | disable}

Function:

Enable/disable the safety IP address authentication on NMS manage station.

Command Mode:

Global Mode

Default:

Enable the safety IP address authentication function.

Example:

Disable the safety IP address authentication function.

```
Switch(config)#snmp-server securityip disable
```

1.4.19 snmp-server view

Command:

snmp-server view <*view-string*> <*oid-string*> {include | exclude}

no snmp-server view <*view-string*> [<*oid-string*>]

Function:

This command is used to create or renew the view information; the “no" form of this command deletes the view information.

Command Mode:

Global Mode.

Parameter:

<*view-string*> view name, containing 1-32 characters.

<*oid-string*>is OID number or corresponding node name, containing 1-255 characters.

include | exclude, include/exclude this OID.

Usage Guide:

The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter.

Example:

Create a view, the name is readview, including iso node but not including the iso.3 node

```
Switch (config)#snmp-server view readview iso include
```

```
Switch (config)#snmp-server view readview iso.3 exclude
```

Delete the view

```
Switch (config)#no snmp-server view readview
```

1.4.20 snmp-server user

Command:

snmp-server user <*use-string*> <*group-string*> [{authPriv | authNoPriv} auth {md5 | sha} <*word*>] [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]

no snmp-server user <*user-string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]

Function:

Add a new user to an SNMP group; the "no" form of this command deletes this user.

Command Mode:

Global Mode.

Parameter:

<user-string> is the user name containing 1-32 characters.

<group-string> is the name of the group the user belongs to, containing 1-32 characters.

authPriv use DES for the packet encryption.

authNoPriv not use DES for the packet encryption.

auth perform packet authentication.

md5 packet authentication using HMAC MD5 algorithm.

sha packet authentication using HMAC SHA algorithm.

<word > user password, containing 8-32 character.

<num-std> is the access-class number for standard numeric ACL, ranging between 1-99;

<name> is the access-class name for standard ACL, the character string length is ranging between 1-32;

<ipv6-num-std> is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

<name> is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.

Usage Guide:

If the encryption and authentication is not selected, the default settings will be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

Example:

Add a new user tester in the UserGroup with an encryption safety level and HMAC md5 for authentication, the password is hellohello

```
Switch (config)#snmp-server user tester UserGroup authPriv auth md5 hellohello
```

deletes an User

```
Switch (config)#no snmp-server user tester
```

1.5 Commands for Switch Upgrade

1.5.1 copy（FTP）

Command:

copy <*source-url*> <*destination-url*> [ascii | binary]

Function:

Download files to the FTP client.

Parameter:

<source-url> is the location of the source files or directories to be copied; ***<destination-url>*** is the destination address to which the files or directories to be copied; forms of ***<source-url>*** and ***<destination-url>*** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission（default transmission method）.When URL represents an FTP address, its form should be: ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>,amongst <*username*> is the FTP user name,<password> is the FTP user password,<ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the FTP server/client,<hostname> is the name of the host mapping with the IPv6 address,it does not support the file download and upload with hosts mapping with IPv4 addresses,<filename> is the name of the FTP upload/download file.

Special keywords of the filename

Keywords **Source or destination addresses**
running-config Running configuration files
startup-config Startup configuration files
nos.img System files
nos.rom System startup files

Command Mode:

Admin Mode.

Usage Guide:

This command supports command line hints, namely if the user can enter commands in following forms: copy <*filename*> ftp:// or copy ftp:// <*filename*> and press Enter, following hints will be provided by the system：

ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

ftp username>

ftp password>

ftp filename>

Requesting for FTP server address, user name, password and file name

Examples:

(1) Save images in the FLASH to the FTP server of 10.1.1.1, FTP server username is Switch, password is superuser

```
Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img
```

(2) Obtain system file nos.img from the FTP server 10.1.1.1, the username is Switch, password is superuser

```
Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img
```

(3) Save images in the FLASH to the FTP server of 2004:1:2:3::6

```
Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img
```

(4) Obtain system file nos.img from the FTP server 2004:1:2:3::6

```
Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration files

```
Switch#copy running-config startup-config
```

Relevant Command:

Write

1.5.2 copy（TFTP）

Command:

copy <*source-url*> <*destination-url*> [ascii | binary]

Function:

Download files to the TFTP client.

Parameter:

<source-url> is the location of the source files or directories to be copied; ***<destination-url>*** is the destination address to which the files or directories to be copied; forms of ***<source-url>*** and ***<destination-url>*** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission（default transmission method）.When URL represents an TFTP address, its form should be: tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>, amongst <ipaddress>| <ipv6address> is the IPv4 or IPv6 address of the TFTP server/client, <*hostname*> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses,<filename> is the name of the TFTP upload/download file.

Special keyword of the filename

Keywords **Source or destination addresses**
running-config Running configuration files
startup-config Startup configuration files
nos.img System files
nos.rom System startup files

Command Mode:

Admin Mode.

Usage Guide:

This command supports command line hints, namely if the user can enter commands in following forms: copy <*filename*> tftp:// or copy tftp:// <*filename*> and press Enter, following hints will be provided by the system:

tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>

tftp filename>

Requesting for TFTP server address, file name

Example:

(1) Save images in the FLASH to the TFTP server of 10.1.1.1

```
Switch#copy nos.img tftp://10.1.1.1/nos.img
```

(2) Obtain system file nos.img from the TFTP server 10.1.1.1

```
Switch#copy tftp://10.1.1.1/nos.img nos.img
```

(3) Save images in the FLASH to the TFTP server of 2004:1:2:3::6

```
Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img
```

(4) Obtain system file nos.img from the TFTP server 2004:1:2:3::6

```
Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration files

```
Switch#copy running-config startup-config
```

Relevant Command:

Write

1.5.3 ftp-dir

Command:

ftp-dir <*ftp-server-url*>

Function:

Browse the file list on the FTP server.

Parameter:

The form of **<ftp-server-url>** is： ftp://<username>:<password>@{ <ipv4address> | <*ipv6address*> }, amongst <*username*> is the FTP user name, <*password*> is the FTP user password, { <ipv4address> | <*ipv6address*> } is the IPv4 or IPv6 address of the FTP server.

Command Mode:

Admin Mode

Example:

Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”

```
Switch#ftp-dir ftp://Switch:superuser @10.1.1.1.
```

1.5.4 ftp-server enable

Command:

ftp-server enable

no ftp-server enable

Function:

Start FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

Default:

FTP server is not started by default.

Command mode:

Global Mode

Usage Guide:

When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not started by default.

Example:

enable FTP server service.

```
Switch#config
Switch(config)# ftp-server enable
```

Relative command:

ip ftp

1.5.5 ftp-server timeout

Command:

ftp-server timeout <*seconds*>

Function:

Set data connection idle time.

Parameter:

<seconds> is the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600.

Default:

The system default is 600 seconds.

Command mode:

Global Mode

Usage Guide:

When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.

Example:

Modify the idle threshold to 100 seconds.

```
Switch#config
Switch(config)#ftp-server timeout 100
```

1.5.6 ip ftp

Command:

ip ftp username <*username*> password [type {0 | 7}] <*password*>

no ip ftp username <*username*>

Function:

Configure the username and password for logging in to the FTP; the no operation of this command will delete the configured username and password simultaneously.

Parameters:

<*username*> is the username of the FTP link, no longer than 16 characters; **0 | 7** represent displaying the password in ciphertext or plaintext; **<*password*>** is the password of the FTP link, no longer than 16 characters.

Default Settings:

the system uses anonymous FTP links by default.

Command Mode:

Global Configuration Mode.

Examples:

Configure the username as Switch and the password as superuser.

```
Switch#
Switch#config
Switch(config)#ip ftp username Switch password 0 superuser
Switch(config)#
```

1.5.7 show ftp

Command:

show ftp

Function:

Display the parameter settings for the FTP server.

Command mode:

Admin and Configuration Mode.

Default:

No display by default.

Example:

```
Switch#show ftp
```

Timeout : 600

Displayed information Description
Timeout Timeout time.

1.5.8 show tftp

Command:

show tftp

Function:

Display the parameter settings for the TFTP server.

Default:

No display by default.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch#show tftp
```

timeout : 60

Retry Times : 10

Displayed information Explanation
Timeout Timeout time.
Retry Times Retransmission times.

1.5.9 tftp-server enable

Command:

tftp-server enable

no tftp-server enable

Function:

Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

Default:

TFTP server is not started by default.

Command mode:

Global Mode

Usage Guide:

When TFTP server function is enabled, the switch can still perform tftp client functions. TFTP server is not started by default.

Example:

Enable TFTP server service.

```
Switch#config
```

```
Switch(config)#tftp-server enable
```

Relative Command:

tftp-server timeout

1.5.10 tftp-server retransmission-number

Command:

tftp-server retransmission-number <*number*>

Function:

Set the retransmission time for TFTP server.

Parameter:

<*number*> is the time to re-transfer, the valid range is 1 to 20.

Default:

The default value is 5 retransmission.

Command mode:

Global Mode

Example:

Modify the retransmission to 10 times.

Switch#config
Switch(config)#tftp-server retransmission-number 10

1.5.11 tftp-server transmission-timeout

Command:

tftp-server transmission-timeout <*seconds*>

Function:

Set the transmission timeout value for TFTP server.

Parameter:

<*seconds*> is the timeout value, the valid range is 5 to 3600s.

Default:

The system default timeout setting is 600 seconds.

Command mode:

Global Mode

Example:

Modify the timeout value to 60 seconds.

Switch#config
Switch(config)#tftp-server transmission-timeout 60

Chapter 2 File System Commands

2.1 cd

Command:

cd <*directory*>

Function:

Change the working directory for the storage device.

Parameters:

<directory> is the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80.

Command Mode:

Admin Mode.

Default Settings:

The default working directory is Flash.

Usage Guide:

After this command implemented, the current storage device will switch to the new working directory, which can be viewed by the “pwd” command.

Example:

Change the working directory of the current storage device to flash.

```
Switch#cd flash：
```

```
Switch#pwd
```

flash:/

```
Switch#
```

2.2 copy

Command:

copy <*source-file-url* > <*dest-file-url*>

Function:

Copy a designated file on the switch and store it as a new file.

Parameters:

<source-file-url> is the source file; ***<dest-file-url>*** is the destination file. When users operate on files stored in backup main-control boardcards and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements.

1. The prefix of the source file URL should be in one of the following forms:
   starting with “flash:/”
   “ftp://username:pass@server-ip/file-name”
   “tftp://server-ip/file-name”
2. The prefix of the destination file URL should be in one of the following forms:
   starting with “flash:/”
   “ftp://username:pass@server-ip/file-name”
   “tftp://server-ip/file-name”

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

1. In this command, when the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.

2. To use this command, the designated source file should exist, and the destination file should not be named the same as any existing directory or file, otherwise, there might be a prompt warning about a failed copy operation or an attempt to overwrite an existing file.

3. If the source and destination files are in different directories, with this command implemented, users can copy files from other directories into the current one.

URL Example: The URL of files in root directory of Flash devices on it should be flash:/nos.img

Example:

Copy the file “flash:/nos.img” and store it as “flash/ 5.2.1.0.img”.

```
Switch#copy flash:/nos.img flash:/nos-5.2.1.0.img
```

Copy flash:/nos.img to flash:/nos-5.2.1.0.img? [Y:N] y

Copyed file flash:/nos.img to flash:/nos-5.2.1.0.img.

2.3 delete

Command:

delete *<file-url>*

Function:

Delete the designate file on the storage device.

Parameters:

<file-url> is the full path of the file to be deleted.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

The designated file will be deleted after implementing this command.

Example:

Delete file flash:/nos.img.

```
Switch#delete flash:/nos5.img
```

Delete file flash:/nos5.img?[Y:N]y

```
Deleted file flash:/nos.img.
```

2.4 dir

Command:

dir [WORD]

Function:

Display the information of the designated directory on the storage device.

Parameters:

<WORD> is the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.

Command Mode:

Admin Configuration Mode.

Default Settings:

No <WORD> means to display information of the current working directory.

Usage Guide:

Implementing this command will display information of files and sub-directories in the designated directory.

Note:

This command does not support a recursive display of all sub-directories.

Example:

Display information of the directory “flash:/”.

```
Switch#dir flash:/
```

```
nos.img          2,449,496          1980-01-01 00:01:06          ----
startup-config   2,064              1980-01-01 00:30:12          ----
Total   7, 932, 928 byte(s)   in   4   file(s)，  free   4, 966, 400 byte(s)
```

```
Switch#
```

2.5 format

Command:

format <*device*>

Function:

Format the storage device.

Parameters:

<device> is the name of the device to be formatted.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

1. After formatting, all files on the storage device will be irrecoverably lost.
2. The only acceptable file system type of Format is FAT 32, without exception.
3. This command cannot be used to format flash.

2.6 mkdir

Command:

mkdir <*directory*>

Function:

Create a sub-directory in the designated directory on a certain storage device .

Parameters:

<directory> is the sub-directory name, a sequence of consecutive characters, whose length ranges from 1 to 80.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

The new created directory should not be named the same as any other directory or file in the designated directory, or located on a flash device. If any error occurs, a prompt will be displayed.

2.7 mount

Command:

mount <*device*>

Function:

Mount the designated device onto the file system.

Parameters:

<device > is the name of the device to be mounted onto the file system.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

The flash's status will automatically be mounted, on which file operations can be implemented.

Example:

Mount the flash card onto the file system.

```
Switch#mount flash：
```

2.8 pwd

Command:

pwd

Function:

Display the current working directory.

Parameters:

None.

Command Mode:

Admin Mode.

Default Settings:

The default directory is flash.

Example:

Display the current working directory.

```
Switch#pwd
```

flash:/
Switch#

2.9 rename

Command:

ename <*source-file-url*> <*new-filename* >

Function:

Rename a designated file on the switch.

Parameters:

<source-file-url>is the source file, in which whether specifying or not its path are both acceptable; ***<new-filename>***is a filename without specifying its path.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.

Example:

Change the name of file “nos.img” in the current working directory to “nos-5.2.1.0.img”.

Switch# rename nos5.img nos-5.2.1.0.img
Rename flash:/nos5.img to flash:/nos-5.2.1.0.img ok !

2.10 rmdir

Command:

rmdir <*directory*>

Function:

Delete a sub-directory in the designated directory on a certain device .

Parameters:

<directory> is the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80.

Command Mode:

Admin Mode.

Default Settings:

None.

Usage Guide:

The directory to be deleted should exist and be empty, that is, all files in the directory should be deleted before deleting it, or an error prompt will be displayed.

2.11 unmount

Command:

unmount <*device*>

Function:

Unmount the designated device from the file system.

Parameters:

<device> is the device to be unmounted from the file system.

Command Mode:

Admin Mode.

Default Settings:

Unmount the FLASH from the file system is nonsupport.

Chapter 3 Commands for Cluster

3.1 clear cluster nodes

Command:

clear cluster nodes [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]

Function:

Clear the nodes in the candidate list found by the commander switch.

Parameters: c

andidate-sn-list: sn of candidate switches, ranging from 1 to 256. More than one candidate can be specified.

mac-address: mac address of the switches (including all candidates, members and other switches).

Default:

No parameter means to clear information of all switches.

Command Mode:

Admin Mode.

Usage Guide:

After executing this command, the information of this node will be deleted from the chain list saved on commander switch. In 30 seconds, the commander will recreate a cluster topology and re-add this node. But after being readded, the candidate id of the switch might change. The command can only be executed on commander switches

Example:

Clear all candidate switch lists found by the commander switch.

```
Switch#clear cluster nodes
```

3.2 cluster auto-add

Command:

cluster auto-add

no cluster auto-add

Function:

When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the "**no cluster auto-add**" command disables this function.

Command mode:

Global Mode

Default:

This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.

Usage Guide：

After enabling this command on a commander switch, candidate switches will be automatically added as members.

Example:

Enable the auto adding function in the commander switch.

```
Switch(config)#cluster auto-add
```

3.3 cluster commander

Command:

cluster commander [<*cluster-name*>]

no cluster commander

Function:

Set the switch as a commander switch, and create a cluster.

Parameter:

<cluster-name> is the cluster's name, no longer than 32 characters.

Command mode:

Global Mode

Default:

Default setting is no commander switch. cluster_name is null by default.

Usage Guide:

This command sets the role of a switch as commander switch and creates a cluster, which can only be executed on non commander switches. The cluster_name cannot be changed after the switch becoming a commander, and "no cluster commander" should be executed first to do that. The no operation of this command will cancel the commander configuration of the switch.

Example:

Set the current switch as the commander switch and name the cluster as switch.

```
Switch(config)#cluster commander switch
```

3.4 cluster ip-pool

Command:

cluster ip-pool <*commander-ip*>

no cluster ip-pool

Function:

Configure private IP address pool for member switches of the cluster.

Parameters：

commander-ip:

cluster IP address pool for allocating internal IP addresses of the cluster commander-ip is the head address of the address pool, of which the valid format is 10.x.x.x, in dotted-decimal notation; the address pool should be big enough to hold 128 members, which requires the last byte of addresses to be less than 126（254 – 128 = 126）. IP address pool should never be changed with commander configured. The change can only be done after the "no cluster commander" command being executed.

Command mode:

Global Mode

Default:

The default address pool is 10.254.254.1.

Usage Guide:

When candidate switches becomes cluster members, the commander switch allocates a private IP address to each member for the communication within the cluster, and thus to realized its management and maintenance of cluster members. This command can only be used on non-commander switches. Once the cluster established, users can not modify its IP address pool. The NO command of this command will restore the address pool back to default value, which is 10.254.254.1.

Example:

Set the private IP address pool used by cluster member devices as 10.254.254.10

```
Switch(config)#cluster ip-pool 10.254.254.10
```

3.5 cluster keepalive interval

Command:

cluster keepalive interval <*second*>

no cluster keepalive interval

Function:

Configure the time interval of keepalive messages within the cluster.

Parameters:

<second>: keepalive time interval, in seconds, ranging from 3 to 30.

Default:

The default value is 30 seconds.

Command Mode:

Global Configuration Mode.

Usage Guide:

After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its keepalive interval is the one distributed by its commander.

Commander will send DP messages within the cluster once in every keepalive interval. Members will respond to the received DP messages with DR messages.

The no operation of this command will restore the keepalive interval in the cluster back to its default value.

Example:

Set the keepalive interval in the cluster to 10 seconds.

```
Switch(config)#cluster keepalive interval 10
```

3.6 cluster keepalive loss-count

Command:

cluster keepalive loss-count<*loss-count*>

no cluster keepalive loss-count

Function:

Configure the max number of lost keepalive messages in a cluster that can be tolerated.

Parameters:

loss-count**:** the tolerable max number of lost messages, ranging from 1 to 10.

Default:

The default value is 3.

Command Mode:

Global Configuration Mode

Usage Guide:

After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its loss-count value is the one distributed by its commander.

commander calculates the loss-count after sending each DP message by adding 1 to the loss-count of each switch and clearing that of a switch after receiving a DR message from the latter. When a loss-count reaches the configured value (3 by default) without receiving any DR message, the commander will delete the switch from its candidate chain list.

If the time that a member fails to receive DP messages from the commander reaches loss-count, it will change its status to candidate.

The no operation of this command will restore the tolerable max number of lost keepalive messages in the cluster back to its default value: 3.

Example:

Set the tolerable max number of lost keepalive messages in the cluster to 5.

```
Switch(config)#cluster keepalive loss-count 5
```

3.7 cluster member

Command:

cluster member {nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*> [id <*member-id*>]}

no cluster member {id <*member-id*> | mac-address <*mac-addr*>}

Function:

On a commander switch, manually add candidate switches into the cluster created by it.

Parameters:

nodes-sn：all cluster member switches as recorded in a chain list, each with a node sn which can be viewed by “show cluster candidates” command. One or more candidates can be added as member at one time. The valid range of candidate-sn-list is 1~256.

mac-address：the CPU Mac of candidate switches

member-id：A member id can be specified to a candidate as it becomes a member, ranging from 1 to 128, increasing from 1 by default.

nodes-sn is the automatically generated sn, which may change after the candidate becomes a member. Members added this way will be actually treated as those added in mac-addr mode with all config files in mac-addr mode.

If more than one switch is added as member simultaneously, no member-id is allowed; neither when using nodes-sn mode.

Default:

None.

Command Mode:

Global Mode

Usage Guide:

After executing this command, the switch will add those identified in ***<nodes-sn>*** or ***<mac-address>***into the cluster it belongs to. One or more candidates are allowed at one time, linked with ‘-‘ or ‘;’. A switch can only be member or commander of one cluster, exclusively. Attempts to execute the command on a non commander switch will return error. The no operation of this command will delete the specified member switch, and turn it back to a candidate.

Example:

In the commander switch, add the candidate switch which has the sequence number as 1. In the commander switch, add the switch whose the mac address is 11-22-33-44-55-66 to member, and the member-id is 5.

```
Switch(config)#cluster member nodes-sn 1
```

```
Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5
```

3.8 cluster member auto-to-user

Command:

cluster member auto-to-user

Function:

All members will be deleted when configuring no cluster auto-add. Users need to change automatically added members to manually added ones to keep them.

Parameter:

None.

Default:

None.

Command Mode:

Global Mode.

Usage Guide:

Execute this command on a switch to change automatically added members to manually added ones.

Example:

change automatically added members to manually added ones.

```
Switch(config)#cluster member auto-to-user
```

3.9 cluster reset member

Command:

cluster reset member [id <*member-id*> | *mac-address <mac-addr>*]

Function:

In the commander switch, this command can be used to reset the member switch.

Parameter:

member-id: ranging from 1 to 128. Use hyphen "-" or semicolon ";" to specify more than one member; if no value is provided, it means to reboot all member switches.

Default:

Boot all member switches.

Command mode:

Admin Mode.

Instructions:

In the commander switch, users can use this command to reset a member switch. If this command is executed in a non-commander switch, an error will be displayed.

Example:

In the commander switch, reset the member switch 1.

```
Switch#cluster reset member 1
```

3.10 cluster run

Command:

cluster run [key <*WORD*>][vid <*VID*>]

no cluster run

Function:

Enable cluster function; the "**no cluster run**" command disables cluster function.

Parameter:

key：all keys in one cluster should be the same, no longer than 16 characters.

vid：vlan id of the cluster, whose range is 1-4094.

Command mode:

Global Mode

Default:

Cluster function is disabled by default, key: NULL(\0) vid：1.

Instructions:

This command enables cluster function. Cluster function has to be enabled before implementing any other cluster commands. The "**no cluster run**" disables cluster function. It is recommended that users allocate an exclusive vlan for cluster（such as vlan100）

Note：Routing protocols should be disabled on the layer-3 interface where cluster vlan locates to avoid broadcasting private route of the cluster.

Example:

Disable cluster function in the local switch.

```
Switch (config)#no cluster run
```

3.11 cluster update member

Command:

cluster update member <*member-id*> <*src-url*> <*dst-filename*> [ascii | binary]

Function:

Remotely upgrade member switches from the commander switch.

Parameters:

member-id：ranging from 1 to 128. Use hyphen "-" or semicolon "；" to specify more than one member;

src-url：the location of source files to be copied;

dst-filename：the specified filename for saving the file in the switch flash;

ascii means that the file transmission follows ASCII standard; binary means that the file transmission follows binary standard, which is de default mode.

when src-url is a FTP address, its form will be: ftp://<username>:<password>@<ipadress>/<filename>，in which <username> is the FTP username <password> is the FTP password <ipadress> is the IP address of the FTP server,<filename> is the name of the file to be downloaded via FTP.

when src-url is a TFTP address, its form will be: tftp://<ipadress>/<filename>，in which <ipadress>is the IP address of the TFTP server <filename> is the name of the file to be downloaded via.

Special keywords used in filename:

Keywords
source or destination address

startup-config start the configuration file
nos.img system file

Command mode:

Admin Mode

Usage Guide:

The commander distributes the remote upgrade command to members via the TCP connections between them, causing the number to implement the remote upgrade and reboot. Trying to execute this command on a non-commander switch will return errors. If users want to upgrade more than one member, these switches should be the same type to avoid boot failure induced by mismatched IMG files.

Example:

Remotely upgrade a member switch from the commander switch, with the member-id being 1, src-ul being ftp://admin:admin@192.168.1.1/nos.img, and dst-url being nos.img

```
Switch#cluster update member 1 ftp://admin:admin@192.168.1.1/nos.img nos.img
```

3.12 debug cluster

Command:

debug cluster {statemachine | application | tcp}

no debug cluster {statemachine | application | tcp}

Function:

Enable the application debug of cluster; the no operation of this command will disable that.

Parameters:

statemachine: print debug information when the switch status changes.

application: print debug information when there are users trying to configure the switch after logging onto it via SNMP, WEB.

tcp: the TCP connection information between the commander members.

Default:

None.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

Enable the debug information of status change on the switch.

```
Swtich#debug cluster statemachine
```

3.13 debug cluster packets

Command:

debug cluster packets {DP | DR | CP} {receive | send}

no debug cluster packets {DP | DR | CP} {receive | send}

Function:

Enable the debug information; the no command disables the debug switch.

Parameters:

DP: discovery messages.

DR: responsive messages.

CP: command messages.

receive: receive messages.

send: send messages.

Default:

None.

Command Mode:

Admin Mode.

Usage Guide:

Enable the debug information of cluster messages. After enabling classification, all DP, DR and CP messages sent or received in the cluster will be printed.

Example:

Enable the debug information of receiving DP messages.

```
Switch#debug cluster packets DP receive
```

3.14 show cluster

Command:

show cluster

Function:

Display cluster information of the switch.

Command Mode:

Admin and Configuration Mode.

Example:

Execute this command on switches of different roles.

----in a commander----------

```
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role:                    commander
IP pool:                 10.254.254.1
Cluster name:            MIS_zebra
Keepalive interval:   30
Keepalive loss-count: 3
Auto add:                Disabled
Number of Members:    0
Number of Candidates: 3
----in a member ----------
Switch#show cluster
Status: Enabled
```

```
Cluster VLAN: 1
Role:     Member
Commander Ip Address: 10.254.254.1
Internal Ip Address:    10.254.254.2
Commamder Mac Address: 00-12-cf-39-1d-90
---- a candidate ---------------------------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role:     Candidate
---- disabled ---------------------------
Switch#show cluster
Status: Disabled
```

3.15 show cluster members

Command:

show cluster members [id <*member-id*> | mac-address <*mac-addr*>]

Function:

Display member information of a cluster. This command can only apply to commander switches.

Parameters:

member-id: member id of the switch.

mac-addr: the CPU mac addresses of member switches.

Default:

No parameters means to display information of all member switches.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

Executing this command on a commander switch will display the configuration information of all cluster member switches.

Example:

Execute this command on a commander switch to display the configuration information of all and specified cluster member switches.

```
Switch#show cluster members
Member From : User config(U); Auto member (A)
ID From Status            Mac                 Hostname       Description     Internal IP
--- - ----------- ----------------- ------------ ------------ ---------------
xxx x xxxxxxxxxx12 xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 xxx.xxx.xxx.xxx
   1 U Inactive        00-01-02-03-04-05 MIS_zebra       DCRS-6804           10.254.254.2
   2 A Active          00-01-02-03-04-05 MIS_bison       DCRS-6804           10.254.254.3
   3 U Active          00-01-02-03-04-05 SRD_jaguar      DCRS-9808           10.254.254.4
   4 A Inactive        00-01-02-03-04-05 HRD_puma        DCRS-5950-28T       10.254.254.5
----
Switch#show cluster members id 1
Cluster Members:
```

```
ID:                1
Member status: Inactive member    (user_config)
IP Address:    10.254.254.2
MAC Address: 00-01-02-03-04-06
Description: DCRS-9808
Hostname:    DSW102
```

3.16 show cluster candidates

Command:

show cluster candidates [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]

Function:

Display the statistic information of the candidate member switches on the command switch

Parameter:

candidate-sn-list：candidate switch sn, ranging from 1 to 256. More than one switch can be specified.

mac-address： mac address of the candidate switch

Default:

No parameters means to display information of all member switches.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

Executing this command on the switch will display the information of the candidate member switches.

Example:

Display configuration information of all cluster candidate switches.

```
Switch#show cluster candidates
Cluster Candidates:
SN          Mac                 Description                    Hostname
--- ----------------- ------------------------ ------------------------
xxx xx-xx-xx-xx-xx-xx xxxxxxxxxxxxxxxxxxxxxx24 xxxxxxxxxxxxxxxxxxxxxx24
   1 00-01-02-03-04-06 XGS3-24040
2 01-01-02-03-04-05 XGS3-24040                        MIS_zebra
```

3.17 show cluster topology

Command:

show cluster topology [root-sn <*starting-node-sn*> | nodes-sn <*node-sn-list*> | mac-address <*mac-addr*>]

Function:

Display cluster topology information. This command only applies to commander switches.

Parameters:

starting-node-sn：the starting node of the topology.

node-sn-list：the switch node sn.

mac-addr：the CPU mac address of the switch.

No parameters means to display all topology information.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

Executing this command on the commander switch will display the topology information with its starting node specified.

Example:

Execute this command on the commander switch to display the topology information under different conditions.

```
Switch#show cluster topology
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)
LV SN Description    Hostname        Role MAC_ADDRESS       Upstream      Upstream
leaf
                                                          local-port    remote-port node
== ============ ============ == ================= ============ ============ =
x xxx xxxxxxxxxx12 xxxxxxxxxx12 xx xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 x
1     1 XGS3-24040         LAB_SWITCH_1 CM 01-02-03-04-05-01 -root-        -root-        -
      2 XGS3-24040         LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1       eth 1/2       N
      3 XGS3-24040         LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/1       eth 1/3       Y
      4 XGS3-24040         LAB_SWITCH_4 CA 01-02-03-04-05-04 eth 1/1       eth 1/4       Y
.....................................................................................
2     2 XGS3-24040         LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1       eth 1/2       -
      5 XGS3-24040         LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1       eth 1/2       Y
      6 XGS3-24040         LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/1       eth 1/3       Y
-------------------------------------------------------------
Switch#show cluster topology root-sn 2
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)
SN Description    Hostname        Role MAC_ADDRESS       Upstream      Upstream
leaf
                                                          local-port    remote-port node
== ============ ============ == ================= ============ ============ =
*     2 XGS3-24040         LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1       eth 1/2       -
      5 XGS3-24040         LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1       eth 1/2       Y
      6 XGS3-24040         LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/1       eth 1/3       Y
-------------------------------------------------
Switch#show cluster topology nodes-sn 2
Toplogy role:    Member
Member status: Active member (user-config)
SN:              2
MAC Address: 01-02-03-04-05-02
Description: XGS3-24040
Hostname     : LAB_SWITCH_2
Upstream local-port: eth 1/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/2
Upstream speed: 100full
Switch#
-----------------------------------------------
Switch#show cluster topology mac-address 01-02-03-04-05-02
```

```
Toplogy role:    Member
Member status: Active member (user-config)
SN:              2
MAC Address: 01-02-03-04-05-02
Description: XGS3-24040
Hostname     : LAB_SWITCH_2
Upstream local-port: eth 1/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/2
Upstream speed: 100full
```

3.18 rcommand commander

Command:

rcommand commander

Function:

In the member switch, use this command to configure the commander switch.

Command mode:

Admin Mode.

Instructions:

This command is used to configure the commander switch remotely. Users have to telnet the commander switch by passing the authentication. The command "**exit**" is used to quit the configuration interface of the commander switch. This command can only be executed on member switches.

Example:

In the member switch, enter the configuration interface of the commander switch.

```
Switch#rcommand commander
```

3.19 rcommand member

Command:

rcommand member *<mem-id>*

Function:

In the commander switch, this command is used to remotely manage the member switches in the cluster.

Parameter:

<mem-id> commander the member id allocated by commander to each member, whose range is 1～128.

Command mode:

Admin Mode.

Usage Guide:

After executing this command, users will remotely login to a member switch and enter Admin Mode on the latter. Use exit to quit the configuration interface of the member. Because of the use of internal private IP, telnet authentication will be omitted on member switches. This command can only be executed on commander switches.

Example:

In the commander switch, enter the configuration interface of the member switch with mem-id 1.

```
Switch#rcommand member 1
```

Chapter 4 Commands for Network Port Configuration

4.1 Commands for Ethernet Port Configuration

4.1.1 bandwidth

Command:

bandwidth control <*bandwidth*> {transmit | receive | both}

no bandwidth control

Function:

Enable the bandwidth limit function on the port; the no command disables this function.

Parameter:

<bandwidth> is the bandwidth limit, which is shown in Mbps ranging between 1-1000000K; **both** refers to the bandwidth limit when the port receives and sends data, **receive** refers to the bandwidth limit will only performed when the switch receives data from out side, while transmit refers to the function will be perform on sending only.

Command Mode:

Port Mode.

Default:

Bandwidth limit disabled by default.

Usage Guide:

When the bandwidth limit is enabled with a size set, the max bandwidth of the port is determined by this size other than by 10/100/1000M. If **[both | receive | transmit]** keyword is not specified, the default is both.

The bandwidth limit can not exceed the physic maximum speed possible on the port. For example, an 10/100M Ethernet port can not be set to a bandwidth limit at 101000K (or higher), but applicable

on a 10/100/1000 port working at a speed of 100M.

Example:

Set the bandwidth limit of 1/1-8 port is 40000K.

```
Switch(config)#interface ethernet 1/1-8
Switch(Config-If-Port-Range)#bandwidth control 40000 both
```

4.1.2 combo-forced-mode

Command:

combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto }

Function:

Sets to combo port mode (combo ports only).

Parameters:

copper-forced forces use of copper cable port; **copper-preferred-auto** for copper cable port first; **sfp-forced** forces use of fiber cable port; **sfp-preferred-auto** for fiber cable port first.

Command mode:

Port Mode.

Default:

The default setting for combo mode of combo ports is fiber cable port first.

Usage Guide:

The combo mode of combo ports and the port connection condition determines the active port of the combo ports. A combo port consists of one fiber port and a copper cable port. It should be noted that the speed-duplex command applies to the copper cable port while the negotiation command applies to the fiber cable port, they should not conflict. For combo ports, only one, a fiber cable port or a copper cable port, can be active at a time, and only this port can send and receive data normally.

For the determination of the active port in a combo port, see the table below. The headline row in the table indicates the combo mode of the combo port, while the first column indicates the connection conditions of the combo port, in which “connected” refers to a good connection of fiber cable port or copper cable port to the other devices.

Copper forced	
Copper preferred	
SFP forced	
SFP preferred	

iber connected, copper not connected Copper cable port Fiber cable port Fiber cable port Fiber cable port
Copper connected, fiber not connected Copper cable port Copper cable port Fiber cable port Copper cable port
Both fiber and copper are connected Copper cable port Copper cable port Fiber cable port Fiber cable port
Neither fiber nor copper are connected Copper cable port Fiber cable port Fiber cable port Fiber cable port

1. Combo port is a conception involving the physical layer and the LLC sublayer of the datalink layer. The status of a combo port will not affect any operation in the MAC sublayer of the datalink layer and upper layers. If the bandwidth limit for a combo port is 1Mbps, then this 1Mbps applies to the active port of this combo port, regardless of the port type being copper or fiber.
2. If a combo port connects to another combo port, it is recommended for both parties to use copper-forced or fiber-forced mode.
3. Run show interface under Admin Mode to check for the active port of a combo port .The following result indicates if the active port for a combo port is the fiber cable port: Hardware is Gigabit-combo, active is fiber.

Example:

Setting ports 1/21-24 to fiber-forced.

```
Switch(config)#interface ethernet 1/21-24
Switch(Config-Port-Range)#combo-forced-mode sfp-forced
```

4.1.3 clear counters interface

Command:

clear counters interface [{ethernet *<interface-list>* | vlan *<vlan-id>* | port-channel *<port-channel-number>* | *<interface-name>*}]

Function:

Clears the statistics of the specified port.

Parameters:

<interface-list> stands for the Ethernet port number; **< *vlan-id* >** stands for the VLAN interface number; ***<port-channel-number>*** for trunk interface number; ***<interface-name>*** for interface name, such as port-channel 1.

Command mode:

Admin Mode.

Default:

Port statistics are not cleared by default.

Usage Guide:

If no port is specified, then statistics of all ports will be cleared.

Example:

Clearing the statistics for Ethernet port1/1.

```
Switch#clear counters interface ethernet 1/1
```

4.1.4 flow control

Command: flow control

no flow control

Function:

Enables the flow control function for the port: the "**no flow control"** command disables the flow control function for the port.

Command mode:

Port Mode.

Default:

Port flow control is disabled by default.

Usage Guide:

After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. Ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Note:

Port flow control function is not recommended unless the users need a slow speed, low performance network with low packet loss. Flow control will not work between different cards in the switch. When enable the port flow control function, speed and duplex mode of both ends should be the same.

Example:

Enabling the flow control function in ports1/1-8.

```
Switch(config)#interface ethernet 1/1-8
Switch(Config-Port-Range)#flow control
```

4.1.5 interface ethernet

Command:

interface ethernet *<interface-list>*

Function:

Enters Ethernet Port Mode from Global Mode.

Parameters:

<interface-list> stands for port number.

Command mode:

Global Mode

Usage Guide:

Run the *exit* command to exit the Ethernet Port Mode to Global Mode.

Example:

Entering the Ethernet Port Mode for ports1/1, 1/4-5, 1/8.

```
Switch(config)#interface ethernet 1/1, 1/4-5, 1/8
Switch(Config-Port-Range)#
```

4.1.6 loopback

Command:

loopback

no loopback

Function:

Enables the loopback test function in an Ethernet port; the "**no loopback**" command disables the loopback test on an Ethernet port.

Command mode:

Port Mode.

Default:

Loopback test is disabled in Ethernet port by default.

Usage Guide:

Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.

Example:

Enabling loopback test in Ethernet ports 1/1-8.

Switch(config)#interface ethernet 1/1-8
Switch(Config-If-Port-Range)#loopback

4.1.7 mdi

Command:

mdi { auto | across | normal }

no mdi

Function:

Sets the cable types supported by the Ethernet port; the "**no mdi**" command sets the cable type to auto-identification. This command is not supported on combo ports and fiber ports.

Parameters:

auto indicates auto identification of cable types; **across** indicates crossover cable support only; **normal** indicates straight-through cable support only.

Command mode:

Port Mode.

Default:

Port cable type is set to auto-identification by default.

Usage Guide:

Auto-identification is recommended. Generally, straight-through cable is used for switch-PC connection and crossover cable is used for switch-switch connection.

Example:

Setting the cable type support of Ethernet ports 1/1-8 to straight-through cable only.

Switch(config)#interface ethernet 1/1-8
Switch(Config-Port-Range)#mdi normal

4.1.8 name

Command:

name <*string*>

no name

Function:

Set name for specified port; the "**no name**" command cancels this configuration.

Parameter:

<string> is a character string, which should not exceeds 32 characters.

Command Mode:

Port Mode.

Default:

No port name by default.

Usage Guide:

This command is for helping the user manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/1-2 ports which is used by financial department, engineering as the name

of 1/9 ports which belongs to the engineering department, while the name of 1/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.

Example:

Specify the name of 1/1-2 port as financial.

Switch(config)#interface ethernet 1/1-2
Switch(Config-If-Port-Range)#name financial

4.1.9 negotiation

Command:

negotiation {on|off}

Function:

Enables/Disables the auto-negotiation function of a 1000Base-FX port.

Parameters:

on: enables the auto-negotiation; off: disable the auto-negotiation.

Command mode:

Port configuration Mode.

Default:

Auto-negotiation is enabled by default.

Usage Guide:

This command applies to 1000Base-FX interface only. The **negotiation** command is not available for 1000Base-TX or 100Base-TX interface. For combo port, this command applies to the 1000Base-FX port only but has no effect on the 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use **speed-duplex** command instead.

Example:

Port 1 of Switch1 is connected to port 1 of Switch2, the following will disable the negotiation for both ports.

Switch1(config)#interface ethernet1/1
Switch1(Config-If-Ethernet1/1)#negotiation off
Switch2(config)#interface ethernet1/1
Switch2(Config-If-Ethernet1/1)#negotiation off

4.1.10 rate-suppression

Command:

rate-suppression {dlf | broadcast | multicast} *<packets>*

no rate-suppression {dlf | broadcast | multicast}

Function:

Sets the traffic limit for broadcasts, multicasts and unknown destination unicasts on all ports in the switch; the no

command disables this traffic throttle function on all ports in the switch, i.e., enables broadcasts, multicasts and unknown destination unicasts to pass through the switch at line speed.

Parameters:

use dlf to limit unicast traffic for unknown destination; multicast to limit multicast traffic; broadcast to limit broadcast traffic. <packets> is the limit of packet number, ranging from 1 to 1488905. For non-10GB ports, the unit of <packets> is PPS, that is, the value of <packets> is the number of packets allowed to pass per second; for 10GB ports, the unit is KPPS, that is, the value of <packets> multiplies 1000 makes the number of packets allowed, so the value should be less than 14880.

Command mode:

Port Mode.

Default:

No limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.

Usage Guide:

All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the above mentioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. Note the difference of this command in 10Gb ports and other ports. If the allowed traffic is set to 3, this means allow 3,120 packets per second and discard the rest for 10Gb ports. However, the same setting for non-10Gb ports means to allow 3 broadcast packets per second and discard the rest.

Example:

Setting ports 8-10 (1000Mbps) allow 3 broadcast packets per second.

Switch(config)#interface ethernet 1/8-10
Switch(Config-Port-Range)#rate-suppression broadcast 3

4.1.11 rate-violation

Command:

rate-violation <packets> [recovery <time>]

no rate-violation

Function:

Enable the limit on packet reception rate function, and set the packet reception rate in one second, the no command delete the function of limit on packet reception rate.

The rate-violation means the packet reception rate, that is, the number of received packets per second, regardless of their type.

Parameters:

<packets> the max number of packets allowed to pass through the port.

recovery: means after a period of time the port can recover “Shutdown” to “UP” again. **<time>** is the timeout of recovery. For example, if the shutdown of a port happens after the packet reception rate exceeding the limit, the port will be “up” again when the user-defined timeout period expires. The default timeout is 300s, while 0 means the recovery will never happen.

Command Mode:

Port Mode

Default:

There is no limit on packet reception rate by default.

Usage Guide:

This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast messages caused by a loop, which affect the processing of other tasks of the switch, the port will be shut down to guarantee the normal operation of the switch.

Example:

If users set the rate-violation of port 8-10 (GB ports) of the switch as 10000pps and the port recovery time as 1200 seconds, when the packet reception rate exceeds 10000, the port will but shut down, and then, after 1200 seconds, the port will be UP again.

Switch(config)#interface ethernet 1/8-10
Switch(Config-Port-Range)#rate-violation 10000 recovery 1200

4.1.12 show interface

Command:

show interface [ethernet *<interface-number>* | port-channel *<port-channel-number>* | loopback *<loopback-id>* | vlan <vlan-id> | tunnel <tunnel-id> | <interface-name>] [detail]

show interface ethernet status

show interface ethernet counter {packet | rate}

Function:

Show information of layer 3 or layer 2 port on the switch

Parameter:

<vlan-id> is the VLAN interface number,the value range from 1 to 4094. <tunnel-number> is the tunnel number, the value range from 1 to 50. <loopback-id> is the loop back number,the value range from 1 to 1024**.** **<interface-number>** is the port number of the Ethernet, status show important information of all the layer 2 ports. counter {packet **|** rate} show package number or rate statistics of all layer 2 ports. ***<port-channel-number>*** is the number of the aggregation interface, ***<interface-name>*** is the name of the interface such as port-channel1. **[detail]** show the detail of the port.

Command Mode:

Admin and Configuration Mode.

Default:

Information not displayed by default

Usage Guide:

While for vlan interfaces, the port MAC address, IP address and the statistic state of the data packet will be shown; for tunnel port, this command will show tunnel interface state and the statistic state of control layer receives/sends tunnel data packet, about the statistic data of physics interface receiving/sending data packet, please refer to show interface ethernet command; for loopback port, this command will show the interface statistic state of IP address and receiving/sending data packet; As for Ethernet port, this command will show port speed rate, duplex mode, flow control switch state, broadcast storm restrain of the port and the statistic state of the data packets; for aggregated port, port speed rate, duplex mode, flow control switch state, broadcast storm restrain of the port and the statistic state of the data packets will be displayed. The information of all ports on the switch will be shown if no port is specified.

Using [detail] to show the detail information for ethernet port and port-channel port, the information is related with the type of switch, board card.

For ethernet port, using status to show important information of all the layer 2 ports by list format. each port is a row,

the showing information include port number, Link, Protocl status, Speed, Duplex, Vlan, port type and port name; counter packets show package number statistics of all ethernet ports, include layer 2 unicast, broadcast, multicast, error of input and output redirection package number; counter rate show the rate statistics of all ethernet ports, input and output package number, byte number in 5 minutes and 5 seconds.

Example:

Show the information of VLAN 1

```
Switch#show interface vlan 1
Vlan1 is up, line protocol is up, dev index is 2005
Device flag 0x1003(UP BROADCAST MULTICAST)
IPv4 address is:
192.168.10.1        255.255.255.0       (Primary)
Hardware is EtherSVI, address is 00-00-00-00-00-01
MTU is 1500 bytes , BW is 0 Kbit
Encapsulation ARPA, loopback not set
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions
```

Show the information of loopback 1:

```
Switch#show interface loopback 1
Loopback1 is up, line protocol is up, dev index is 2006
Device flag 0x100b(UP BROADCAST LOOP MULTICAST)
IPv4 address is:
1.1.1.1 255.255.255.255 (Primary)
MTU is 1500 bytes , BW is 0 Kbit
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
```

```
0 output errors, 0 collisions
```

Sshow the information of tunnel 1:

```
Switch#show interface tunnel 1
Tunnel1 is up, line protocol is up, dev index is 2007
Device flag 0x91(UP P2P NOARP)
IPv4 address is:
(NULL)
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions
```

Show the information of port 1/1:

```
Switch#show interface e1/1
Ethernet1/1 is up, line protocol is down
Ethernet1/1 is layer 2 port, alias name is (null), index is 1
Hardware is Gigabit-TX, address is 00-30-4f-02-fc-01
PVID is 1
MTU 1500 bytes, BW 10000 Kbit
Encapsulation ARPA, Loopback not set
Auto-duplex: Negotiation half-duplex, Auto-speed: Negotiation 10M bits
FlowControl is off, MDI type is auto
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
0 input packets, 0 bytes, 0 no buffer
0 unicast packets, 0 multicast packets, 0 broadcast packets
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored
0 abort, 0 length error, 0 pause frame
Output packets statistics:
0 output packets, 0 bytes, 0 underruns
0 unicast packets, 0 multicast packets, 0 broadcast packets
0 output errors, 0 collisions, 0 pause frame
```

Show the important information of all layer 2 ports:

```
Switch#show interface ethernet status
Codes: A-Down - administratively down, a - auto, f - force, G - Gigabit
Interface Link/Protocol Speed Duplex Vlan Type Alias Name
1/1 UP/UP f-100M f-full 1 G-TX
1/2 UP/UP a-100M a-full trunk G-TX
1/3 UP/DOWN auto auto 1 G-TX
1/4 A-Down/DOWN auto auto 1 G-TX
```

Show the package number statistics information of all layer 2 ports:

```
Switch#Show interface ethernet counter packet
Interface Unicast(pkts) BroadCast(pkts) MultiCast(pkts) Err(pkts)
1/1 IN 12,345,678 12,345,678,9 12,345,678,9 4,567
OUT 23,456,789 34,567,890 5,678 0
1/2 IN 0 0 0 0
OUT 0 0 0 0
1/3 IN 0 0 0 0
OUT 0 0 0 0
1/4 IN 0 0 0 0
OUT 0 0 0 0
…
```

Show the rate statistics information of all layer 2 ports:

```
Switch # Show interface ethernet counter rate
Interface IN(pkts/s) IN(bytes/s) OUT(pkts/s) OUT(bytes/s)
1/1 5m 13,473 12,345,678 12,345 1,234,567
5s 135 65,800 245 92,600
1/2 5m 0 0 0 0
5s 0 0 0 0
1/3 5m 0 0 0 0
5s 0 0 0 0
1/4 5m 0 0 0 0
5s 0 0 0 0
```

4.1.13 shutdown

Command:

shutdown

no shutdown

Function:

Shuts down the specified Ethernet port; the "**no shutdown**" command opens the port.

Command mode:

Port Mode.

Default:

Ethernet port is open by default.

Usage Guide:

When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the "**show interface**" command is "down".

Example:

Opening ports1/1-8.

```
Switch(config)#interface ethernet1/1-8
Switch(Config-Port-Range)#no shutdown
```

4.1.14 speed-duplex

Command:

speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected | no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}}

no speed-duplex

Function:

Sets the speed and duplex mode for 1000Base-TX, 100Base-TX or 100Base-FX ports; the "**no speed-duplex**" command restores the default speed and duplex mode setting, i.e., auto speed negotiation and duplex.

Parameters:

auto for auto speed negotiation; **force10-half** for forced 10Mbps at half-duplex; **force10-full** for forced 10Mbps at full-duplex mode; **force100-half** for forced 100Mbps at half-duplex mode; **force100-full** for forced 100Mbps at full-duplex mode; **force100-fx** for forced 100Mbps at full-duplex mode; **module-type** is the type of 100Base-FX module; **auto-detected:** automatic to detect; **no-phy-integrated:** there is no phy-integratd 100Base-TX module; **phy-integrated:** phy-integratd 100Base-TX module; **force1g-half** for forced 1000Mbps at half-duplex mode; **force1g-full** for forced 1000Mbps at full-duplex mode; **nonegotiate** for disable auto-negotiation for 1000 Mb port; **master** to force the 1000Mb port to be **master** mode; **slave** to force the 1000Mb port to be **slave** mode.

Command mode:

Port Mode.

Default:

Auto-negotiation for speed and duplex mode is set by default.

Usage Guide:

This command is configures the port speed and duplex mode. When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

1000Gb ports are by default **master** when configuring **nonegotiate** mode. If one end is set to **master** mode, the other end must be set to **slave** mode.

force1g-half is not supported yet.

Example:

Port 1 of SwitchA is connected to port 1 of SwitchB, the following will set both ports in forced 100Mbps at half-duplex mode.

SwitchA(config)#interface ethernet1/1
SwitchA(Config-If-Ethernet1/1)#speed-duplex force100-half
SwitchB(config)#interface ethernet1/1
SwitchB(Config-If-Ethernet1/1)#speed-duplex force100-half

Chapter 5 Commands for Port Isolation Function

5.1 isolate-port group

Command:

isolate-port group <*WORD*>

no isolate-port group <*WORD*>

Function:

Set a port isolation group, which is the scope of isolating ports; the no operation of this command will delete a port isolation group and remove all ports out of it.

Parameters:

<*WORD*> is the name identification of the group, no longer than 32 characters.

Command Mode:

Global Mode.

Default:

None.

Usage Guide:

Users can create different port isolation groups based on their requirements. For example, if a user wants to isolate all downlink ports in a vlan of a switch, he can implement that by creating a port isolation group and adding all downlink ports of the vlan into it. No more than 16 port isolation groups can a switch have. When the users need to change or redo the configuration of the port isolation group, he can delete the existing group with the no operation of this command.

Example:

Create a port isolation group and name it as ”test”.

Switch>enable
Switch#config
Switch(config)#isolate-port group test

5.2 isolate-port group switchport interface

Command:

isolate-port group <*WORD*> switchport interface [ethernet] <*IFNAME*>

no isolate-port group <WORD> switchport interface [ethernet] <*IFNAME*>

Function:

Add one port or a group of ports into a port isolation group to isolate, which will become isolated from the other ports in the group. The no operation of this command will remove one port or a group of ports out of a port isolation group, which will be able to communicate will ports in that group normally. If the ports removed from the group still belong to another port isolation group, they will remain isolated from the ports in that group. If an Ethernet port is a member of a convergence group, it should not be added into a port isolation group, and vice versa, a member of a port isolation group should not be added into an aggregation group. But one port can be a member of one or more port isolation groups.

Parameters:

<WORD> is the name identification of the group, no longer than 32 characters. If there is no such group with the specified name, create one; **ethernet** means that the ports to be isolated is Ethernet ones, followed by a list of Ethernet ports, supporting symbols like ";" and "-". For example: "ethernet 1/1;3;4-7;8" ***<IFNAME>*** is the name of the interface, such as e1/1. If users use interface name, the parameter of ethernet will not be required.

Command Mode:

Global Mode.

Default:

None.

Usage Guide:

Users can add Ethernet ports into or remove them from a port isolation group according to their requirements. When an Ethernet port is a member of more than one port isolate group, it will be isolated from every port of all groups it belongs to.

Example:

Add Ethernet ports 1/1-2 and 1/5 into a port isolation group named as "test".

```
Switch(config)#isolate-port group test switchport interface ethernet 1/1-2; 1/5
```

5.3 isolate-port apply

Command:

isolate-port apply [*<l2|l3|all>*]

Function:

This command will apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows.

Parameters:

<l2|l3|all> the flow to be isolated, l2 means isolating layer-2 flows, l3 means isolating layer-3 flows, all means isolating all flows.

Command Mode:

Global Mode.

Default:

Isolate all flows.

Usage Guide:

User can apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows according to their requirements.

Example:

Only apply port isolation to layer-2 flows on the switch.

```
Switch(config)#isolate-port apply l2
```

5.4 show isolate-port group

Command:

show isolate-port group [<*WORD*>]

Function:

Display the configuration of port isolation, including all configured port isolation groups and Ethernet ports in each group.

Parameters:

<WORD> the name identification of the group, no longer than 32 characters; no parameter means to display the configuration of all port isolation groups.

Command Mode:

Admin Mode and Global Mode.

Default:

Display the configuration of all port isolation groups.

Usage Guide:

Users can view the configuration of port isolation with this command.

Example:

Display the port isolation configuration of the port isolation group named as “test”.

```
Switch(config)#show isolate-port group test
Isolate-port group test
    The isolate-port Ethernet1/5
    The isolate-port Ethernet1/2
```

Chapter 6 Commands for Port Loopback Detection Function

6.1 loopback-detection control

Command:

loopback-detection control {shutdown |block| learning}

no loopback-detection control

Function:

Enable the function of loopback detection control on a port, the no operation of this command will disable the function.

Parameters:

shutdown set the control method as shutdown, which means to close down the port if a port loopback is found.

block set the control method as block, which means to block a port by allowing bpdu and loopback detection messages only if a port loopback is found.

learning disable the control method of learning MAC addresses on the port, not forwarding traffic and delete the MAC address of the port.

Default:

Disable the function of loopback diction control.

Command Mode:

Port Mode.

Usage Guide:

If there is any loopback, the port will not recovery the state of be controlled after enabling control operation on the port. If the overtime is configured, the ports will recovery normal state when the overtime is time-out. If the control method is block, the corresponding relationship between instance and vlan id should be set manually by users, it should be noticed when be used.

Example:

Enable the function of loopback detection control under port1/2 mode.

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#loopback-detection control shutdown
Switch(Config-If-Ethernet1/2)#no loopback-detection control

6.2 loopback-detection specified-vlan

Command:

loopback-detection specified-vlan <*vlan-list*>

no loopback-detection specified-vlan [<*vlan-list*>]

Function:

Enable the function of loopback detection on the port and specify the VLAN to be checked; the no operation of this command will disable the function of detecting loopbacks through this port or the specified VLAN.

Parameters:

<*vlan-list*> the list of VLANs allowed passing through the port. Given the situation of a trunk port, the specified VLANs can be checked. So this command is used to set the vlan list to be checked.

Default:

Disable the function of detecting the loopbacks through the port.

Command Mode:

Port Mode.

Usage Guide:

If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This function is not supported under Port-channel.

Example:

Enable the function of loopback detection under port 1/2 mode.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#switchport mode trunk
Switch(Config-If-Ethernet1/2)#switchport trunk allowed vlan all
Switch(Config-If-Ethernet1/2)#loopback-detection specified-vlan 1;3;5-20
Switch(Config-If-Ethernet1/2)#no loopback-detection specified-vlan 1;3;5-20
```

6.3 loopback-detection interval-time

Command:

oopback-detection interval-time *<loopback> <no-loopback>*

no loopback-detection interval-time

Function:

Set the loopback detection interval. The no operate closes the loopback detection interval function.

Parameters:

<loopback > the detection interval if any loopback is found, ranging from 5 to 300, in seconds.

<no-loopback > the detection interval if no loopback is found, ranging from 1 to 30, in seconds.

Default:

The default value is 5s with loopbacks existing and 3s otherwise.

Command Mode:

Global Mode.

Usage Guide:

When there is no loopback detection, the detection interval can be relatively shorter, for too short a time would be a disaster for the whole network if there is any loopback. So, a relatively longer interval is recommended when loopbacks exist.

Example:

Set the loopback diction interval as 35, 15.

```
Switch(config)#loopback-detection interval-time 35 15
```

6.4 loopback-detection control-recovery timeout

Command:

loopback-detection control-recovery timeout <0-3600>

Function:

This command is used to recovery to uncontrolled state after a special time when a loopback being detected by the port entry be controlled state.

Parameters:

<0-3600> second is recovery time for be controlled state, 0 is not recovery state.

Default:

The recovery is not automatic by default.

Command Mode:

Global Configuration Mode.

Usage Guide:

When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.

Examples:

Enable automatic recovery of the loopback-detection control mode after 30s.

```
Switch(config)#loopback-detection control-recovery timeout 30
```

6.5 show loopback-detection

Command:

show loopback-detection [interface <*interface-list*>]

Function:

Display the state of loopback detection on all ports if no parameter is provided, or the state and result of the specified ports according to the parameters.

Parameters:

<interface-list> the list of ports to be displayed, for example: ethernet 1/1.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

Display the state and result of loopback detection on ports with this command.

Example:

Display the state of loopback detection on port 4.

```
Switch(config)#show loopback-detection interface Ethernet 1/4
loopback detection config and state information in the switch!
PortName            Loopback Detection          Control Mode    Is Controlled
Ethernet1/4         Enable                      Shutdown        No
```

6.6 debug loopback-detection

Command:

debug loopback-detection

Function:

After enabling the loopback detection debug on a port, BEBUG information will be generated when sending, receiving messages and changing states.

Parameters:

None.

Command Mode:

Admin Mode.

Default:

Disabled by default.

Usage Guide:

Display the message sending, receiving and state changes with this command.

Example:

```
Switch#debug loopback-detection
%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev Ethernet1/10, vlan id 1
%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev Ethernet 1/10, vlan id 2
```

Chapter 7 Commands for ULDP

7.1 uldp enable

Command:

uldp enable

Function:

ULDP will be enabled after issuing this command. In global configuration mode, this command will enable ULDP for the global. In port configuration mode, this command will enable ULDP for the port.

Parameters:

None.

Command Mode:

Global Configuration Mode and Port Configuration Mode.

Default:

By default ULDP is not configured.

Usage Guide:

ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.

Example:

To enable ULDP in global configuration mode.

```
Switch(config)#uldp enable
```

7.2 uldp disable

Command:

uldp disable

Function:

To disable ULDP configuration through this command.

Parameters:

None.

Command Mode:

Global Configuration Mode and Port Configuration Mode.

Default:

By default ULDP is not configured.

Usage Guide:

When ULDP is disabled globally, then ULDP in all the ports will be disabled.

Example:

To disable the ULDP configuration in global configuration mode.

```
Switch(config)#uldp disable
```

7.3 uldp hello-interval

Command:

uldp hello-interval <*integer*>

no uldp hello-interval

Function:

To configure the interval for ULDP to send hello messages. The no form of this command will restore the default interval for the hello messages.

Parameters:

The interval for the Hello messages, with its value limited between 5 and 100 seconds, 10 seconds by default.

Command Mode:

Global Configuration Mode.

Default:

10 seconds by default.

Usage Guide:

Interval for hello messages can be configured only if ULDP is enabled globally, its value limited between 5 and 100 seconds.

Example:

To configure the interval of Hello messages to be 12 seconds.

```
Switch(config)# uldp hello-interval 12
```

7.4 uldp aggressive-mode

Command:

uldp aggressive-mode

no uldp aggressive-mode

Function:

To configure ULDP to work in aggressive mode. The no form of this command will restore the normal mode.

Parameters:

None.

Command Mode:

Global Configuration Mode and Port Configuration Mode.

Default:

Normal mode.

Usage Guide:

The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in port configuration mode.

Example:

To enable ULDP aggressive mode globally.

```
Switch(config)# uldp aggressive-mode
```

7.5 uldp manual-shutdown

Command:

uldp manual-shutdown

no uldp manual-shutdown

Function:

To configure ULDP to work in manual shutdown mode. The no command will restore the automatic mode.

Parameters:

None.

Command Mode:

Global Configuration Mode.

Default:

Auto mode.

Usage Guide:

This command can be issued only if ULDP has been enabled globally.

Example:

To enable manual shutdown globally.

```
Switch(config)# uldp manual-shutdown
```

7.6 uldp reset

Command:

uldp reset

Function:

To reset the port when ULDP is shutdown.

Parameters:

None.

Command Mode:

Globally Configuration Mode and Port Configuration Mode.

Default:

None.

Usage Guide:

This command can only be effect only if the specified interface is disabled by ULDP.

Example:

To reset all the port which are disabled by ULDP.

```
Switch(config)# uldp reset
```

7.7 uldp recovery-time

Command:

uldp recovery-time<*integer*>

no uldp recovery-time

Function:

To configure the interval for ULDP recovery timer. The no form of this command will restore the default configuration.

Parameters:

recovery-time is the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.

Command Mode:

Global Configuration Mode.

Default:

0 is set by default which means the recovery is disabled.

Usage Guide:

If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.

Example:

To set the recovery timer to be 600 seconds.

```
Switch(config)# uldp recovery-time 600
```

7.8 show uldp

Command:

show uldp [interface ethernet<*interface-name*>]

Function:

To show the global ULDP configuration and status information of interface. If <interface-name> is specified, ULDP configuration and status about the specified interface as well as its neighbors' will be displayed.

Parameters:

<interface-name>is the interface name.

Command Mode:

Admin and Configuration Mode.

Default:

None.

Usage Guide:

If no parameters are appended, the global ULDP information will be displayed. If the interface name is specified, information about the interface and its neighbors will be displayed along with the global information.

Example:

To display the global ULDP information.

```
Switch(config)# show uldp
```

7.9 debug uldp fsm interface ethernet

Command:

debug uldp fsm interface ethernet *<IFname>*

no debug uldp fsm interface ethernet *<IFname>*

Function:

To enable debugging information for ULDP for the specified interface. The no form of this command will disable the debugging information.

Parameters:

<IFname> is the interface name.

Command Mode:

Admin Configuration Mode.

Default:

Disabled by default.

Usage Guide:

This command can be used to display the information about state transitions of the specified interfaces.

Example:

Print the information about state transitions of interface ethernet 1/1.

```
Switch#debug uldp fsm interface ethernet 1/1
```

7.10 debug uldp error

Command:

debug uldp error

no debug uldp error

Function:

Enable the error message debug function, the no form command disable the function.

Parameter:

None.

Command Mode:

Admin Mode.

Default:

Disabled.

Usage Guide:

Use this command to display the error message.

Example:

Display the error message.

```
Switch#debug uldp error
```

7.11 debug uldp event

Command:

debug uldp event

no debug uldp event

Function:

Enable the message debug function to display the event; the no form command disables this function.

Parameter:

None.

Command Mode:

Admin Mode.

Default:

Disabled.

Usage Guide:

Use this command to display all kinds of event information.

Example:

Display event information.

```
Switch# debug uldp event
```

7.12 debug uldp packet

Command:

debug uldp packet [receive|send]

no debug uldp packet [receive|send]

Function:

Enable receives and sends packet debug function, after that. Display the type and interface of the packet which receiving and sending on the client. The no form command disables this function.

Parameter:

None.

Command Mode:

Admin Mode.

Default:

Disabled.

Usage Guide:

Use this command to display the packet that receiving on each interface.

```
Switch# debug uldp packet receive
```

7.13 debug uldp interface ethernet

Command:

debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <*IFname*>

no debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <*IFname*>

Function:

Enable the debug function of display the packet details. After that, display some kinds of the packet details of terminal interface.

Parameter:

***<IFname>*:** Name of the interface.

Command Mode:

Admin Mode.

Default:

Disabled.

Usage Guide:

Use this command to display the Hello packet details receiving on the interface Ethernet 1/1.

```
Switch# debug uldp hello receive interface Ethernet 1/1
```

Chapter 8 Commands for LLDP Function

8.1 lldp enable

Command:

lldp enable

lldp disable

Function:

Globally enable LLDP function; the no operation of this command globally disables LLDP function.

Parameters:

None.

Default:

Disable LLDP function.

Command Mode:

Global Mode.

Usage Guide:

If LLDP function is globally enabled, it will be enabled on every port.

Example:

Enable LLDP function on the switch.

```
Switch(config)# lldp enable
```

8.2 lldp enable (Port)

Command:

lldp enable

lldp disable

Function:

Enable the LLDP function module of ports in port configuration mode; the no operation of this command will disable the LLDP function module of port.

Parameters:

None.

Default:

the LLDP function module of ports is enabled by default in port configuration mode.

Command Mode:

Port Configuration Mode.

Usage Guide:

When LLDP is globally enabled, it will be enabled on every port, the switch on a port is used to disable this function when it is unnecessary on the port.

Example:

Disable LLDP function of port on the port ethernet 1/5 of the switch.

```
Switch(config)#in ethernet 1/5
```

```
Switch(Config-if-ethernet 1/5)#lldp disable
```

8.3 lldp mode

Command: l

ldp mode <*send*|*receive*|*both*|*disable*>

Function:

Configure the operating state of LLDP function of the port.

Parameters:

send: Configure the LLDP function as only being able to send messages.

receive: Configure the LLDP function as only being able to receive messages.

both: Configure the LLDP function as being able to both send and receive messages.

disable: Configure the LLDP function as not being able to send or receive messages.

Default:

The operating state of the port is “both”.

Command Mode:

Port Configuration Mode.

Usage Guide:

Choose the operating state of the lldp Agent on the port.

Example:

Configure the state of port ethernet 1/5 of the switch as “receive”.

```
Switch(config)#in ethernet 1/5
```

```
Switch(Config-if-Ethernet 1/5)#lldp mode receive
```

8.4 lldp tx-interval

Command:

lldp tx-interval <*integer*>

no lldp tx-interval

Function:

Set the interval of sending update messages on all the ports with LLDP function enabled, the value of which ranges from 5 to 32768 seconds and is 30 seconds by default.

Parameters:

<*seconds*>is the interval of sending updating messages, ranging from 5 to 32768 seconds.

Default:

30 seconds.

Command Settings:

Global Mode.

Usage Guide:

After configuring the interval of sending messages, LLDP messages can only be received after a

period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often; while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds.

When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.

Example:

Set the interval of sending messages as 40 seconds.

```
Switch(config)# lldp tx-interval 40
```

8.5 lldp msgTxHold

Command:

lldp msgTxHold <*value*>

no lldp msgTxHold

Function:

Set the multiplier value of the aging time carried by update messages sent by the all ports with LLDP function enabled, the value ranges from 2 to 10.

Parameters:

<*value*> is the aging time multiplier, ranging from 2 to 10.

Default:

the value of the multiplier is 4 by default.

Command Mode:

Global Mode.

Usage Guide:

After configuring the multiplier, the aging time is defined as the product of the multiplier and the interval of sending messages, and its maximum value is 65535 seconds.

Example:

Set the value of the aging time multiplier as 6.

```
Switch(config)#lldp msgTxHold 6
```

8.6 lldp transmit delay

Command:

lldp transmit delay <*seconds*>

no lldp transmit delay

Function:

Since local information might change frequently because of the variability of the network environment, there could be many update messages sent in a short time. So a delay is required to guarantee an accurate statistics of local information.

When transmit delay is the default value and tx-interval is configured via some commands, transmit delay will become one fourth of the latter, instead of the default 2.

Parameters:

<seconds>is the time interval, ranging from 1 to 8192 seconds.

Default:

The interval is 2 seconds by default.

Command Mode:

Global Mode.

Usage Guide:

When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.

Example:

Set the delay of sending messages as 3 seconds.

```
Switch(config)# lldp transmit delay 3
```

8.7 lldp notification interval

Command:

lldp notification interval <*seconds*>

no lldp notification interval

Function:

When the time interval ends, the system is set to check whether the Remote Table has been changed. If it has, the system will send Trap to the SNMP management end.

Parameters:

<seconds>is the time interval, ranging from 5 to 3600 seconds.

Default:

The time interval is 5 seconds.

Command Mode:

Global Mode.

Usage Guide:

After configuring the notification time interval, a “trap” message will be sent at the end of this time interval whenever the Remote Table changes.

Example:

Set the time interval of sending Trap messages as 20 seconds.

```
Switch(config)# lldp notification interval 20
```

8.8 lldp trap

Command:

lldp trap <*enable*|*disable*>

Function:

enable: configure to enable the Trap function on the specified port;

disable: configure to disable the Trap function on the specified port.

Parameters:

None.

Default:

The Trap function is disabled on the specified port by default.

Command Mode:

Port Configuration Mode.

Usage Guide:

The function of sending Trap messages is enabled on the port.

Example:

Enable the Trap function on port ethernet 1/5 of the switch.

Switch(config)#in ethernet 1/5
Switch(Config-if-ethernet 1/5)# lldp trap enable

8.9 lldp transmit optional tlv

Command:

lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]

no lldp transmit optional tlv

Function:

Configure the type of optional TLV of the port.

Parameters:

portDesc: the description of the port; **sysName:** the system name; **sysDesc:** The description of the system; **sysCap:** the capability of the system.

Default:

The messages carry no optional TLV by default.

Command Mode:

Port Configuration Mode.

Usage Guide:

When configuring the optional TLV, each TLV can only appear once in a message, **portDesc** optional TLV represents the name of local port; **sysName** optional TLV represents the name of local system; **sysDesc** optional TLV represents the description of local system; **sysCap** optional TLV represents the capability of local system.

Example:

Configure that port ethernet 1/5 of the switch carries portDesc and sysCap TLV.

Switch(config)#in ethernet 1/5
Switch(Config-if-ethernet 1/5)# lldp transmit optional tlv portDesc sysCap

8.10 lldp neighbors max-num

Command:

lldp neighbors max-num < *value* >

no lldp neighbors max-num

Function:

Set the maximum number of entries can be stored in Remote MIB.

Parameters:

<value> is the configured number of entries, ranging from 5 to 500.

Default:

The maximum number of entries can be stored in Remote MIB is 100.

Command Mode:

Port Configuration Mode.

Usage Guide:

The maximum number of entries can be stored in Remote MIB.

Example:

Set the Remote as 200 on port ethernet 1/5 of the switch.

Switch(config)#in ethernet 1/5
Switch(Config-if-ethernet 1/5)# lldp neighbors max-num 200

8.11 lldp tooManyNeighbors

Command:

lldp tooManyNeighbors {discard|delete}

Function:

Set which operation will be done when the Remote Table is full.

Parameters:

discard: discard the current message.

delete: Delete the message with the least TTL in the Remoter Table.

Default:

Discard.

Command Mode:

Port Configuration Mode.

Usage Guide:

When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.

Example:

Set port ethernet 1/5 of the switch as delete.

Switch(config)#in ethernet 1/5
Switch(Config-if-ethernet 1/5)# lldp tooManyNeighbors delete

8.12 show lldp

Command:

show lldp

Function:

Display the configuration information of global LLDP, such as the list of all the ports with LLDP enabled, the interval of sending update messages, the configuration of aging time, the interval needed by the sending module to wait for re-initialization, the interval of sending TRAP, the limitation of the number of the entries in the Remote Table.

Parameters:

None.

Default:

Do not display the configuration information of global LLDP.

Command Mode:

Admin Mode, Global Mode.

Usage Guide:

Users can check all the configuration information of global LLDP by using “show lldp”.

Example:

Check the configuration information of global LLDP after it is enabled on the switch.

```
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP enabled port : Ethernet 1/1
LLDP interval :30
LLDP txTTL :120
LLDP txShutdownWhile :2
LLDP NotificationInterval :5
LLDP txDelay :20
-------------END------------------
```

8.13 show lldp traffic

Command:

show lldp traffic

Function:

Display the statistics of LLDP data packets.

Parameters:

None.

Default:

Do not display the statistics of LLDP data packets.

Command Mode:

Admin Mode, Global Mode.

Usage Guide:

Users can check the statistics of LLDP data packets by using “show lldp traffic”.

Example:

Check the statistics of LLDP data packets after LLDP is enabled on the switch.

```
Switch(config)#show lldp traffic
PortName      Ageouts      FramesDiscarded      FramesInErrors      FramesIn      FramesOut
TLVsDiscarded    TLVsUnrecognized ----------      -------      ---------------      --------------
--------      ---------      -------------      ----------------
Ethernet1/1      0                0                    0                0             7                0
0
```

8.14 show lldp interface ethernet

Command:

show lldp interface ethernet <*IFNAME*>

Function:

Display the configuration information of LLDP on the port, such as: the working state of LLDP Agent.

Parameters:

***<IFNAME>*:** Interface name.

Default:

Do not display the configuration information of LLDP on the port.

Command Mode:

Admin Mode, Global Mode.

Usage Guide:

Users can check the configuration information of LLDP on the port by using “show lldp interface ethernet XXX”.

Example:

Check the configuration information of LLDP on the port after LLDP is enabled on the switch.

```
Switch(config)#show lldp interface ethernet 1/1
Port name:     ethernet 1/1
  LLDP Agent Adminstatus: Both
  LLDP Operation TLV: portDecs   sysName   sysDesc   sysCap
  LLDP Trap Status: disable
  LLDP maxRemote: 100
  LLDP Overflow handle: discard
LLDP interface remote status : Full
```

8.15 show lldp neighbors interface ethernet

Command:

show lldp neighbors interface ethernet < *IFNAME* >

Function:

Display the LLDP neighbor information of the port.

Parameters:

None.

Default:

Do not display the LLDP neighbor information of the port.

Command Mode:

Admin Mode, Global Mode.

Usage Guide:

Users can check the LLDP neighbor information of the port by using “show lldp neighbors interface ethernet XXX”.

Example:

Check the LLDP neighbor information of the port after LLDP is enabled on the port.

```
Switch(config)#show lldp neighbors interface ethernet 1/1
```

8.16 show debugging lldp

Command:

show debugging lldp

Function:

Display all ports with lldp debug enabled.

Parameters:

None.

Default:

None.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

With show debugging lldp, all ports with lldp debug enabled will be displayed.

Example:

Display all ports with lldp debug enabled.

```
Switch(config)#show debugging lldp
====BEGINNING OF    LLDP DEBUG SETTINGS====
debug lldp
debug lldp packets interface Ethernet1/1
debug lldp packets interface Ethernet1/2
debug lldp packets interface Ethernet1/3
debug lldp packets interface Ethernet1/4
debug lldp packets interface Ethernet1/5
=============END OF DEBUG SETTINGS===============
```

8.17 debug lldp

Command:

debug lldp

no debug lldp

Function:

Enable the debug information of LLDP function, the no operation of this command will disable the debug information of LLDP function.

Parameters:

None.

Default:

Disable the debug information of LLDP function.

Command Mode:

Admin Mode.

Usage Guide:

When the debug switch is enabled, users can check the receiving and sending of packets and other information.

Example:

Enable the debug switch of LLDP function on the switch.

```
Switch(config)#debug lldp
```

8.18 debug lldp packets

Command:

debug lldp packets interface ethernet <*IFNAME*>

no debug lldp packets interface ethernet <*IFNAME*>

Function:

Display the message-receiving and message-sending information of LLDP on the port; the no operation of this command will disable the debug information switch.

Parameters:

None.

Default:

Disable the debug information on the port.

Command Mode:

Admin Mode.

Usage Guide:

When the debug switch is enabled, users can check the receiving and sending of packets and other information on the port.

Example:

Enable the debug switch of LLDP function on the switch.

```
Switch(config)# debug lldp packets interface ethernet 1/1
```

```
%Jan 01 00:02:40 2006 LLDP-PDU-TX      PORT= ethernet 1/1.
```

8.19 clear lldp remote-table

Command:

clear lldp remote-table

Function:

Clear the Remote-table on the port.

Parameters:

None.

Default:

Do not clear the entries.

Command Mode:

Port Configuration Mode.

Usage Guide:

Clear the Remote table entries on this port.

Example:

Clear the Remote table entries on this port.

```
Switch(Config-Ethernet 1/1)# clear lldp remote-table
```

Chapter 9 Commands for Port Channel

9.1 debug port-channel

Command:

debug port-channel <*port-group-number*> {all | event | fsm | packet | timer}

no debug port-channel [<*port-group-number*>]

Function:

Open the debug switch of port-channel.

Parameters:

<port-group-number> is the group number of port channel, ranging from 1 to 128

all: all debug information

event: debug event information

fsm: debug the state machine

packet: debug LACP packet information

timer: debug the timer information

Command mode:

Admin mode.

Default:

Disable the debugging of port-channel.

Usage Guide:

Open the debug switch to check the debug information of port-channel.

Example:

(1)debug the state machine for port-group 1.

```
Switch#debug port-channel 1 fsm
```

(2) debug LACP packet information for port-group 2.

```
Switch#debug port-channel 2 packet
```

(3) debug all for port-group 1.

```
Switch#debug port-channel 1 all
```

9.2 interface port-channel

Command:

interface port-channel <*port-channel-number*>

Function:

Enters the port channel configuration mode

Command mode:

Global Mode

Usage Guide:

On entering aggregated port mode, configuration to GVRP or spanning tree modules will apply to aggregated ports; if the aggregated port does not exist (i.e., ports have not been aggregated), an error message will be displayed and configuration will be saved and will be restored until the ports are aggregated. Note such restoration will be performed only once, if an aggregated group is ungrouped and aggregated again, the initial user configuration will not be restored. If it is configuration for modules, such as shutdown configuration, then the configuration to current port will apply to all member ports in the corresponding port group.

Example:

Entering configuration mode for port-channel 1.

```
Switch(config)#interface port-channel 1
```

```
Switch(Config-If-Port-Channel1)#
```

9.3 lacp port-priority

Command:

lacp port-priority <*port-priority*>

no lacp port-priority

Function:

Set the port priority of LACP protocol.

Parameters: <*port-priority*>:

the port priority of LACP protocol, the range from 0 to 65535.

Command mode:

Port Mode.

Default:

The default priority is 32768 by system.

Usage Guide:

Use this command to modify the port priority of LACP protocol, the no command restores the default value.

Example:

Set the port priority of LACP protocol.

```
Switch(Config-If-Ethernet1/1)# lacp port-priority 30000
```

9.4 lacp system-priority

Command:

lacp system-priority <*system-priority*>

no lacp system-priority

Function:

Set the system priority of LACP protocol.

Parameters:

***<system-priority>*:** The system priority of LACP protocol, ranging from 0 to 65535.

Command mode:

Global Mode

Default:

The default priority is 32768.

Usage Guide:

Use this command to modify the system priority of LACP protocol, the no command restores the default value.

Example:

Set the system priority of LACP protocol.

```
Switch(config)# lacp system-priority 30000
```

9.5 load-balance

Command:

load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip}

Function:

Set load-balance mode for port-group.

Parameter:

src-mac performs load-balance according to the source MAC

dst-mac performs load-balance according to the destination MAC

dst-src-mac performs load-balance according to the source and destination MAC

src-ip performs load-balance according to the source IP

dst-ip performs load-balance according to the destination IP

dst-src-ip performs load-balance according to the destination and source IP

Command mode:

Aggregation port mode.

Default:

Perform load-balance according to the source and destination MAC.

Usage Guide:

Use port-channel to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode of port-group, then modify the load-balance of port-group as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.

Example:

Set load-balance mode of port-group.

```
Switch(config)#interface port-channel 1
```

```
Switch(Config-If-Port-Channel1)# load-balance src-mac
```

9.6 port-group

Command:

port-group <*port-group-number*> }]

no port-group <*port-group-number*>

Function:

Creates a port group. The no command deletes that group.

Parameters:

<port-group-number> is the group number of a port channel from 1 to 128.

Default:

There is no port-group.

Command mode:

Global Mode

Example:

Creating a port group.

```
Switch(config)# port-group 1
```

Delete a port group.

```
Switch(config)#no port-group 1
```

9.7 port-group mode

Command:

port-group <*port-group-number*> mode {active|passive|on}

no port-group

Function:

Add a physical port to port channel, the no operation removes specified port from the port channel.

Parameters:

<port-group-number> is the group number of port channel, from 1 to 128;

active enables LACP on the port and sets it in Active mode;

passive enables LACP on the port and sets it in Passive mode; **on** forces the port to join a port channel without enabling LACP.

Command mode:

Port Mode.

Default:

Switch ports do not belong to a port channel by default; LACP not enabled by default.

Usage Guide:

If the specified port group does not exist, then print a error message. All ports in a port group must be added in the same mode, i.e., all ports use the mode used by the first port added. Adding a port in “on” mode is a “forced” action, which means the local end switch port aggregation does not rely on the information of the other end, port aggregation will succeed as long as all ports have consistent VLAN information. Adding a port in “active” or “passive” mode enables LACP. Ports of at least one end must be added in “active” mode, if ports of both ends are added in “passive” mode, the ports will never aggregate.

Example:

Under the Port Mode of Ethernet1/1, add current port to “port-group 1” in “active” mode.

```
Switch(Config-If-Ethernet1/1)#port-group 1 mode active
```

9.8 show port-group

Command:

show port-group [<*port-group-number*>] {brief | detail |}

Function:

Display the specified group number or the configuration information of all port-channel which have been configured.

Parameters:

<port-group-number> is the group number of port channel to be displayed, from 1 to 128;

brief displays summary information;

detail displays detailed information.

Command mode:

All Configuration Mode.

Default:

None.

Usage Guide:

If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.

Example:

1. Display the summary information of port-group 1.

```
Switch# show port-group brief
ID: port group number;   Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
          first one is select ports number, last one is unselect ports number.

ID    Mode       Partner ID                    Ports   load-balance
------------------------------------------------------------
1     on         0x8000,00e0-fcff-ff01      1,0      src-ip
10    active     none                          1,1      dst-mac
20    passive    0x8000,0041-f3fc-3431      1,1      dst-src-ip
```

2. Display the detailed information of port-group 1.

```
Switch#show port-group 1 detail
Flags:   A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
         D -- Synchronization, E -- Collecting, F -- Distributing,
         G -- Defaulted, H -- Expired
```

```
Port-group number: 1,   Mode: on,     Load-balance: src-ip
Port-group detail information:
System ID: 0x8000, 000f-e219-57c3
Port Status: S -- Selected,   U -- Unselected
Local:
  Port              Status   Priority   Oper-Key   Flag
-------------------------------------------------------------
  Ethernet1/2       S        32768      2          {ACDEF}
  Ethernet1/3       S        32768      2          {ACDEF}

Remote:
  Actor           Partner Priority   Oper-Key   SystemID                  Flag
-------------------------------------------------------------------------------
  Ethernet1/2     161       32768        1          0x8000,00e0-fc00-12b0   {ACDEF}
  Ethernet1/3     164       32768        1          0x8000,00e0-fc00-12b0   {ACDEF}
```

Chapter 10 Commands for Jumbo

10.1 jumbo enable

Command:

jumbo enable [<mtu-value>]

no jumbo enable

Function:

Enable the Jumbo receiving function. The no command restores to the normal frame range of 64--1518。

Parameter:

mtu-value: the MTU value of jumbo frame that can be received, in byte, ranging from <1500-9000>. The corresponding frame size is <1518/1522-9018/9022>. Without setting is parameter, the allowed max frame size is 9018/9022.

Default:

Jumbo function not enabled by default.

Command Mode:

Global Mode

Usage Guide:

Set switch of both ends jumbo necessarily, or jumbo frame will be dropped at the switch has not be set.

Example:

Enable the jumbo function of the switch.

```
Switch(config)#jumbo enable
```

Chapter 11 VLAN Configuration

11.1 Commands for VLAN Configuration

11.1.1 debug gvrp

Command:

debug gvrp

no debug gvrp

Function:

Enable the GVRP debugging function: the “no debug gvrp” command disables the function.

Command mode:

Admin Mode.

Default:

GVRP debug information is disabled by default.

Usage Guide:

Use this command to enable GVRP debugging, GVRP packet processing information can be displayed.

Example:

Enable GVRP debugging.

```
Switch#debug gvrp
```

11.1.2 dot1q-tunnel enable

Command:

dot1q-tunnel enable

no dot1q-tunnel enable

Function:

Set the access port of the switch to dot1q-tunnel mode; the “**no dot1q-tunnel enable**” command restores to default.

Parameter:

None.

Command Mode:

Port Mode.

Default:

Dot1q-tunnel function disabled on the port by default.

Usage Guide:

After enabling dot1q-tunnel on the port, data packets without VLAN tag (referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is 8100 and the VLAN ID is the VLAN ID the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports, and also on trunk ports however only when associating the VLAN translation function. This command and dot1q-tunnel tpid are

mutually exclusive.

Example:

Join port1 into VLAN3, enable dot1q-tunnel function.

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-If-Ethernet1/1)# exit
Switch(config)#
```

11.1.3 dot1q-tunnel tpid

Command:

dot1q-tunnel tpid {0x8100|0x9100|0x9200| <1-65535> }

Function:

Configure the type (TPID) of the protocol of switch trunk port.

Parameter:

None.

Command Mode:

Port Mode.

Default:

TPID on the port is defaulted at 0x8100.

Usage Guide:

This function is to facilitate internetworking with equipments of other manufacturers. If the equipment connected with the switch trunk port sends data packet with a TPID of 0x9100, the port TPID will be set to 0x9100, this way switch will receive and process data packets normally. This command and dot1q-tunnel enable are mutually exclusive.

Example:

Set port10 of the switch to trunk port and sends data packet with a TPID of 0x9100.

```
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/10)#dot1q-tunnel tpid 0x9100
```

Switch(Config-If-Ethernet1/10)#exit
Switch(config)#

11.1.4 gvrp

Command:

gvrp

no gvrp

Function:

Enable the GVRP function for the switch or the current Trunk port; the "**no gvrp**" command disables the GVRP function globally or for the port.

Command mode:

Port Mode and Global Mode.

Default:

GVRP is disabled by default.

Usage Guide:

Port GVRP can only be enabled after global GVRP is enabled. When global GVRP is disabled, the GVRP configurations in the ports are also disabled. Note: GVRP can only be enabled on Trunk ports.

Example:

Enable the GVRP function globally and for Trunk port 10.

Switch(config)#gvrp
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#gvrp
Switch(config)#exit

11.1.5 garp timer hold

Command:

garp timer hold <*timer-value*>

no garp timer hold

Function:

Set the hold timer for GARP; the "**no garp timer hold**" command restores the default timer setting.

Parameter:

<timer-value> is the value for GARP hold timer, the valid range is 100 to 327650 ms.

Command mode:

Port Mode.

Default:

The default value for hold timer is 100 ms.

Usage Guide:

When GARP application entities receive a join message, join message will not be sent immediately. Instead, hold timer is started. After hold timer timeout, all join messages received with the hold time will be sent in one GVRP frame, thus effectively reducing protocol message traffic.

Example:

Set the GARP hold timer value of port 1/10 to 500 ms.

```
Switch(Config-If-Ethernet1/10)#garp timer hold 500
```

11.1.6 garp timer join

Command:

garp timer join <*timer-value*>

no garp timer join

Function:

Set the join timer for GARP; the "**no garp timer join**" command restores the default timer setting.

Parameter:

<timer-value> is the value for join timer, the valid range is 100 to 327650 ms.

Command mode:

Port Mode.

Default:

The default value for join timer is 200 ms.

Usage Guide:

GARP application entity sends a join message after join timer over, other GARP application entities received the join message will register this message.

Example:

Set the GARP join timer value of port 10 to 1000 ms.

```
Switch(Config-If-Ethernet1/10)#garp timer join 1000
```

11.1.7 garp timer leave

Command:

garp timer leave <*timer-value*>

no garp timer leave

Function:

Set the leave timer for GARP; the "**no garp timer leave**" command restores the default timer setting.

Parameter:

<timer-value>is the value for leave timer, the valid range is 100 to 327650 ms.

Command mode:

Port Mode.

Default:

The default value for leave timer is 600 ms.

Usage Guide:

When GARP application entity wants to cancel a certain property information, it sends a leave message. GARP application entities receiving this message will start the leave timer, if no join message is received before leave timer timeout, the property information will be canceled. Besides, the value of leave timer must be twice larger than the join timer. Otherwise, an error message will be displayed.

Example:

Set the GARP leave timer value of port 1/10 to 3000 ms.

```
Switch(Config-If-Ethernet1/10)#garp timer leave 3000
```

11.1.8 garp timer leaveall

Command:

garp timer leaveall <*timer-value*>

no garp timer leaveall

Function:

Set the leaveall timer for GARP; the "**no garp timer leaveall**" command restores the default timer setting.

Parameter:

<timer-value> is the value for GARP leaveall timer, the valid range is 100 to 327650 ms.

Command mode:

Global Mode.

Default:

The default value for leaveall timer is 10000 ms.

Usage Guide:

When a GARP application entity starts, the leaveall timer is started at the same time. When the leaveall timer is over, the GARP application entity will send a leaveall message. Other application entities will cancel all property information for that application entity, and the leaveall timer is cleared for a new cycle.

Example:

Set the GARP leaveall timer value to 50000 ms.

```
Switch(config)#garp timer leaveall 50000
```

11.1.9 name

Command:

name <*vlan-name*>

no name

Function:

Specify a name, a descriptive string, for the VLAN; the no operation of the command will delete the name of the VLAN.

Parameters:

<vlan-name> is the specified name string.

Command Mode:

VLAN Configuration Mode.

Default:

The default VLAN name is vlanXXX, where xxx is VID.

Usage Guide:

The switch can specify names for different VLANs, making it easier for users to identify and manage VLANs.

Examples:

Specify the name of VLAN100 as TestVlan.

```
Switch(Config-Vlan100)#name TestVlan
```

11.1.10 private-vlan

Command:

private-vlan {primary | isolated | community}

no private-vlan

Function:

Configure current VLAN to Private VLAN. The "**no private-vlan**" command cancels the Private VLAN configuration.

Parameter:

primary set current VLAN to Primary VLAN,

isolated set current VLAN to Isolated VLAN,

community set current VLAN to Community VLAN.

Command Mode:

VLAN mode

Default:

Private VLAN is not configured by default.

Usage Guide:

There are three Private VLANs: **Primary** VLAN, **Isolated** VLAN and **Community** VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.

Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.

It is to be noted Private VLAN messages will not be transmitted by GVRP.

Example:

Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types.

```
Switch(config)#vlan 100
```

```
Switch(Config-Vlan100)#private-vlan primary
```

Note:This will remove all the ports from vlan 100

```
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
```

Note:This will remove all the ports from vlan 200

```
Switch(Config-Vlan200)#exit
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
```

Note:This will remove all the ports from vlan 300

```
Switch(Config-Vlan300)#exit
```

11.1.11 private-vlan association

Command:

private-vlan association <*secondary-vlan-list*>

no private-vlan association

Function:

Set Private VLAN association; the "**no private-vlan association**" command cancels Private VLAN association.

Parameter:

<secondary-vlan-list> Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ";".

Command mode:

VLAN Mode.

Default:

There is no Private VLAN association by default.

Usage Guide:

This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN.

Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

Example:

Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

```
Switch(Config-Vlan100)#private-vlan association 200;300
```

11.1.12 show dot1q-tunnel

Command:

show dot1q-tunnel

Function:

Display the information of all the ports at dot1q-tunnel state.

Parameter:

None.

Command Mode:

Admin Mode and other configuration Mode.

Usage Guide:

This command is used for displaying the information of the ports at dot1q-tunnel state.

Example:

Display current dot1q-tunnel state.

```
Switch#show dot1q-tunnel
```

Interface Ethernet1/1:

dot1q-tunnel is enable

I nterface Ethernet1/3:

dot1q-tunnel is enable

11.1.13 show garp

Command:

show garp [<*interface-name*>]

Function:

Display the global and port information for GARP.

Parameter:

<interface-name> stands for the name of the Trunk port to be displayed.

Command mode:

Admin Mode and other configuration Mode.

Usage Guide:

N/A.

Example:

Display global GARP information.

```
Switch #show garp
```

11.1.14 show gvrp

Command:

show gvrp [<*interface-name*>]

Function:

Display the global and port information for GVRP.

Parameter:

<interface-name> stands for the name of the Trunk port to be displayed.

Command mode:

Admin Mode and other configuration Mode.

Usage Guide:

N/A.

Example:

Display global GVRP information.

```
Switch#show gvrp configuration
---------- Gvrp Information ----------
Gvrp status : enable
Gvrp Timers(milliseconds)
LeaveAll      :   10000
```

11.1.15 show vlan

Command:

show vlan [brief | summary] [id <*vlan-id*>] [name <*vlan-name*>] [internal usage [id <*vlan-id*> | name <*vlan-name*>]] [private-vlan [id <*vlan-id*> | name <*vlan-name*>]]

Function:

detailed information for all VLANs or specified VLAN.

Parameter:

brief stands for brief information; **summary** for VLAN statistics; ***<vlan-id>*** for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; ***<vlan-name>*** is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters. **private-vlan** displays the ID, name, relating VLAN and port of the private-vlan relative information.

Command mode:

Admin Mode and configuration Mode.

Usage Guide:

If no ***<vlan-id>*** or ***<vlan-name>*** is specified, then information for all VLANs in the switch will be displayed.

Example:

Display the status for the current VLAN; display statistics for the current VLAN.

```
Switch#show vlan
VLAN Name              Type        Media       Ports
---- ------------ ---------- --------- ----------------------------------------
1    default        Static      ENET      Ethernet1/1  Ethernet1/2
                                          Ethernet1/3    Ethernet1/4
                                          Ethernet1/9    Ethernet1/10
```

```
                                        Ethernet1/11    Ethernet1/12
2      VLAN0002        Static        ENET          Ethernet1/5     Ethernet1/6
                                        Ethernet1/7     Ethernet1/8
Switch#show vlan summary
The max. vlan entrys: 4094
Existing Vlans:
Universal Vlan:
1 12 13 15 16 22
Total Existing Vlans is:6

Switch(config)#show vlan private-vlan
VLAN Name        Type    Asso    VLAN    Ports
---- ------------ ---------- --------- ----------------------------------------
100    VLAN0100    Primary    101     102      Ethernet6/9        Ethernet6/10
                                        Ethernet6/11        Ethernet6/12
                                        Ethernet6/13
101    VLAN0101    Community 100           Ethernet6/9        Ethernet6/10
                                        Ethernet6/11        Ethernet6/12
                                        Ethernet6/13
102   VLAN0102     Isolate      100         Ethernet6/9
```

Displayed information Explanation
VLAN VLAN number
Name VLAN name
Type VLAN type, statically configured or dynamically learned.
Media VLAN interface type: Ethernet
Ports Access port within a VLAN

11.1.16 show vlan-translation

Command:

show vlan-translation

Function:

Display the information of all the ports at VLAN-translation state.

Parameter:

None.

Command Mode:

Admin Mode and other configuration Mode.

Usage Guide:

Display the information of all the ports at VLAN-translation state, including enabling, packet dropped, direction and other information.

Example:

Display current VLAN translation state information.

```
Switch#show vlan-translation
Interface Ethernet1/1:
    vlan-translation is enable, miss drop is set in
Interface Ethernet1/2:
    vlan-translation is enable, miss drop is not set
Interface Ethernet1/3:
    vlan-translation is enable, miss drop is set both
```

11.1.17 switchport access vlan

Command:

switchport access vlan <*vlan-id*>

no switchport access vlan

Function:

Add the current Access port to the specified VLAN. The "**no switchport access vlan**" command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

Parameter:

<vlan-id> is the VID for the VLAN to be added the current port, valid range is 1 to 4094.

Command mode:

Port Mode.

Default:

All ports belong to VLAN1 by default.

Usage Guide:

Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

Example:

Add some Access port to VLAN100.

```
Switch(config)#interface ethernet 1/8
Switch(Config-If-Ethernet1/8)#switchport mode access
Switch(Config-If-Ethernet1/8)#switchport access vlan 100
Switch(Config-If-Ethernet1/8)#exit
```

11.1.18 switchport hybrid allowed vlan

Command:

switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag}no switchport hybrid allowed vlan

Function:

Set hybrid port which allow the VLAN to pass with tag or untag method; the "**no switchport hybrid allowed vlan**" command restores the default setting.

Parameter:

WORD: Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;

all: Set all VLANs to allowed vlan;

add WORD: Add vlanList to the existent allowed vlanList;

except WORD: Set all VLANs to allowed vlan except the configured vlanList;

remove WORD: Delete the specific VLAN of vlanList from the existent allow vlanList;

tag: Join the specific VLAN with tag mode;

untag: Join the specific VLAN with untag mode.

Command mode:

Port Mode.

Default:

Deny all VLAN traffic to pass.

Usage Guide:

The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the before.

Example:

Set hybrid port allowed vlan 1, 3, 5-20 with untag mode and allow vlan 100; 300; 500-2000 with tag mode.

Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/5)#switchport hybrid allowed vlan 1;3;5-20 untag
Switch(Config-If-Ethernet1/5)#switchport hybrid allowed vlan 100; 300; 500-2000 tag
Switch(Config-If-Ethernet1/5)#exit

11.1.19 switchport hybrid native vlan

Command:

switchport hybrid native vlan <*vlan-id*>

no switchport hybrid native vlan

Function:

Set the PVID for Hybrid port; the "**no switchport hybrid native vlan**" command restores the default setting.

Parameter:

<vlan-id> is the PVID of Hybrid port.

Command mode:

Port Mode.

Default:

The default PVID of Hybrid port is 1.

Usage Guide:

When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

Example:

Set the native vlan to 100 for a Hybrid port.

Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/5)#switchport hybrid native vlan 100
Switch(Config-If-Ethernet1/5)#exit

11.1.20 switchport interface

Command:

switchport interface [ethernet | portchannel] [interface-name | interface-list]

no switchport interface [ethernet | portchannel] [interface-name | interface-list]

Function:

Specify Ethernet port to VLAN; the "**no switchport interface [ethernet | portchannel] [<*interface-name* | *interface-list*>]**" command deletes one or one set of ports from the specified VLAN.

Parameter:

ethernet is the Ethernet port to be added. **portchannel** means that the port to be added is a link-aggregation port. **interface-name** port name, such as e1/1. If this option is selected, ethernet or portchannel should not be. **interface-list** is the port list to be added or deleted, ";" and "-" are supported, for **example:**

ethernet1/1;3;4-7;8.

Command mode:

VLAN Mode.

Default:

A newly created VLAN contains no port by default.

Usage Guide:

Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

Example:

Assign Ethernet port 1, 3, 4-7, 8 of VLAN100.

```
Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8
```

11.1.21 switchport mode

Command:

switchport mode {trunk | access | **hybrid}**

Function:

Set the port in access mode, trunk mode or hybrid mode.

Parameter:

trunk means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only; hybrid means the port allows the traffic of multi-VLANs to pass with tag or untag mode.

Command mode:

Port Mode.

Default:

The port is in Access mode by default.

Usage Guide:

Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly

convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

Example:

Set port 5 to trunk mode and port 8 to access mode, port 10 to hybrid mode.

Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#exit
Switch(config)#interface ethernet 1/8
Switch(Config-If-Ethernet1/8)#switchport mode access
Switch(Config-If-Ethernet1/8)#exit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/10)#exit

11.1.22 switchport trunk allowed vlan

Command:

switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD}

no switchport trunk allowed vlan

Function:

Set trunk port to allow VLAN traffic; the "**no switchport trunk allowed vlan**" command restores the default setting.

Parameter:

WORD: specified VIDs; keyword;

all: all VIDs, the range from 1 to 4094;

add: add assigned VIDs behind **allow vlan**;

except: all VID add to **allow vlan** except assigned VIDs;

remove: delete assigned **allow vlan** from **allow vlan** list.

Command mode:

Port Mode.

Default:

Trunk port allows all VLAN traffic by default.

Usage Guide:

The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited.

Example:

Set Trunk port to allow traffic of VLAN1, 3, 5-20.

Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet1/5)#exit

11.1.23 switchport trunk native vlan

Command:

switchport trunk native vlan <*vlan-id*>

no switchport trunk native vlan

Function:

Set the PVID for Trunk port; the "**no switchport trunk native vlan**" command restores the default setting.

Parameter:

<vlan-id> is the PVID for Trunk port.

Command mode:

Port Mode.

Default:

The default PVID of Trunk port is 1.

Usage Guide:

PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When a untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this commands for VLAN forwarding.

Example:

Set the native VLAN for a Trunk port to 100.

Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet1/5)#exit

11.1.24 vlan

Command:

vlan WORD

no vlan WORD

Function:

Create VLANs and enter VLAN configuration mode. If using ';' and '-' connect with multi-VLANs, then only create these VLANs. If only existing VLAN, then enter VLAN configuration mode; if the VLAN is not exist, then create VLAN and enter VLAN configuration mode. In VLAN Mode, the user can set VLAN name and assign the switch ports to the VLAN. The no command deletes specified VLANs.

Parameter:

WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ';' and '-'.

Command mode:

Global Mode.

Default:

Only VLAN1 is set by default.

Usage Guide:

VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.

Example:

Create VLAN100 and enter the configuration mode for VLAN 100.

Switch(config)#vlan 100
Switch(Config-Vlan100)#

11.1.25 vlan-translation

Command:

vlan-translation <*old-vlan-id*> to <*new-vlan-id*> {in|out}

no vlan-translation <*old-vlan-id*> {in|out}

Function:

Add VLAN translation by creating a mapping between original VLAN ID and current VLAN ID; the “no” form of this command deletes corresponding mapping.

Parameter:

old-vlan-id is the original VLAN ID;new-vlan-id is the translated VLAN ID; in indicates entrance translation; out indicates exit translation.

Command Mode:

Port Mode.

Default:

The command is for configuring the in and out translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while the vlan-translation miss drop command will determine the next forwarding if not match. Same original VLAN ID and same current VLAN ID can be configured in different directions, however, the original and the current VLAN ID must not be the same.

Example:

Move the VLAN100 data entered from the port1 to VLAN2 after entrance translation, and the data traffic out from VLAN2 to VLAN100 after exit translation.

Switch#config
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#dot1q-tunnel enable
Switch(Config-If-Ethernet1/1)#vlan-translation enable
Switch(Config-If-Ethernet1/1)#vlan-translation 100 to 2 in
Switch(Config-If-Ethernet1/1)#vlan-translation 2 to 100 out
Switch(Config-If-Ethernet1/1)#exit
Switch(config)#

11.1.26 vlan-translation enable

Command:

vlan-translation enable

no vlan-translation enable

Function:

Enable VLAN translation on specified trunk port of the switch; the "**no vlan-translation enable**" command restores to the default value.

Parameter:

None.

Command Mode:

Port Mode.

Default:

VLAN translation has not been enabled on the port by default.

Usage Guide:

To apply VLAN translation on the port the dot1q-tunnel function must be first enabled and configured at trunk port.

Example:

Enable VLAN translation function on port1.

```
Switch#config
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#dot1q-tunnel enable
Switch(Config-If-Ethernet1/1)#vlan-translation enable
```

11.1.27 vlan-translation miss drop

Command:

vlan-translation miss drop{in|out|both}

no vlan-translation miss drop{in|out|both}

Function:

Set to packet dropping upon translation failure; the “no” form of this command restores to the default value.

Parameter:

In refers to entrance; out indicates exit; both represents bidirectional .

Command Mode:

Port Mode.

Default:

No packet dropping upon translation failure by default.

Usage Guide:

When performing the mapping translation between the original and the current VID, if no translation correspondence is configured, the packet will not be dropped by default, but will after use this command.

Example:

Set to packet dropped at entrance of port1 when translation fails.

```
Switch(Config-If-Ethernet1/1)#vlan-translation miss drop in
```

11.1.28 vlan ingress enable

Command:

vlan ingress enable

no vlan ingress enable

Function:

Enable the VLAN ingress rule for a port; the "**no vlan ingress enable**" command disables the ingress rule.

Command mode:

Port Mode.

Default:

VLAN ingress rules are enabled by default.

Usage Guide:

When VLAN ingress rules are enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is a VLAN member port.

Example:

Disable VLAN ingress rules on the port.

```
Switch(Config-If-Ethernet1/1)# no vlan ingress enable
```

11.2 Commands for Dynamic VLAN Configuration

11.2.1 dynamic-vlan mac-vlan prefer

Command:

dynamic-vlan mac-vlan prefer

Function:

Set the MAC-based VLAN preferred.

Parameter:

None.

Command Mode:

Global Mode.

Default:

MAC-based VLAN is preferred by default.

Usage Guide:

Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command.

Example:

Set the MAC-based VLAN preferred.

```
SwitchA#config
SwitchA(config)#dynamic-vlan mac-vlan prefer
```

11.2.2 dynamic-vlan subnet-vlan prefer

Command:

dynamic-vlan subnet-vlan prefer

Function:

Set the IP-subnet-based VLAN preferred.

Parameter:

None.

Command Mode:

Global Mode.

Default:

MAC-based VLAN is preferred by default.

Usage Guide:

Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN.

Example:

Set the IP-subnet-based VLAN preferred.

Switch#config
Switch(config)#dynamic-vlan subnet-vlan prefer

11.2.3 mac-vlan

Command:

mac-vlan mac <*mac-addrss*> vlan <*vlan-id*> priority <*priority-id*>

no mac-vlan {mac <*mac-addrss*>|all}

Function:

Add the correspondence between MAC address and VLAN, namely specify certain MAC address to join specified VLAN. The “no” form of this command deletes all/the correspondence.

Parameter:

mac-address is the MAC address which is shown in the form of XX-XX-XX-XX-XX-XX,vlan-id is the ID of the VLAN with a valid range of 1~4094;priority-id is the level of priority and is used in the VLAN tag with a valid range of 0~7;all refers to all the MAC addresses.

Command Mode:

Global Mode.

Default:

No MAC address joins the VLAN by default.

Usage Guide:

With this command user can add specified MAC address to specified VLAN. If there is a non VLAN label data packet enters from the switch port from the specified MAC address, it will be assigned with specified VLAN ID so sent enter specified VLAN. Their belonging VLAN are the same no matter which port did they enter through. The command does not have any interfere on the VLAN label data packet.

Example:

Add network device of MAC address as 00-30-4f-11-22-33 to VLAN 100.

Switch#config
Switch(config)#mac-vlan mac 00-30-4f-11-22-33 vlan 100 priority 0

11.2.4 mac-vlan vlan

Command:

mac-vlan vlan <*vlan-id*>

no mac-vlan vlan <*vlan-id*>

Function:

Configure the specified VLAN to MAC VLAN; the “**no mac-vlan vlan <*vlan-id*>**” command cancels the MAC VLAN configuration of this VLAN.

Parameter:

<*vlan-id*> is the number of the specified VLAN.

Command Mode:

Global Mode.

Default:

No MAC VLAN is configured by default.

Usage Guide:

Set specified VLAN for MAC VLAN, There can be only one MAC VLAN at the same time.

Example:

Set VLAN100 to MAC VLAN.

Switch#config
Switch(config)#mac-vlan vlan 100

11.2.5 protocol-vlan

Command:

protocol-vlan mode {ethernetii etype <*etype-id*> | llc {dsap <*dsap-id*> ssap <*ssap-id*>} | snap etype <*etype-id*>} vlan <*vlan-id*> priority <*priority-id*>

no protocol-vlan {mode {ethernetii etype <*etype-id*> | llc {dsap <*dsap-id*> ssap <*ssap-id*>} | snap etype <*etype-id*>} | all}

Function:

Add the correspondence between the protocol and the VLAN namely specify the protocol to join specified VLAN. The “no” form of this command deletes all/the correspondence.

Parameter:

mode is the encapsulate type of the configuration which is ethernetii, llc, snap; the encapsulate type of the ethernetii is EthernetII;

etype-id is the type of the packet protocol, with a valid range of 1536~65535;

llc is LLC encapsulate format;

dsap-id is the access point of the destination service, the valid range is 0~255;

ssap-id is the access point of the source service with a valid range of 0~255;

snap is SNAP encapsulate format;

etype-id is the type of the packet protocol, the valid range is 1536~65535;

vlan-id is the ID of VLAN, the valid range is 1~4094;

priority is the priority, the range is 0~7;

all indicates all the encapsulate protocols.

Command Mode:

Global Mode.

Default:

No protocol joined the VLAN by default.

Usage Guide:

The command adds specified protocol into specified VLAN. If there is any non VLAN label packet from specified protocol enters through the switch port, it will be assigned with specified VLAN ID and enter the specified VLAN. No matter which port the packets go through, their belonging VLAN is the same. The command will not interfere with VLAN labeled data packets. It is recommended to configure ARP protocol together with the IP protocol or else some application may be affected.

Example:

Assign the IP protocol data packet encapsulated by the EthernetII to VLAN200.

Switch#config
Switch(config)#protocol-vlan mode ethernetii etype 2048 vlan 200

11.2.6 show dynamic-vlan prefer

Command:

show dynamic-vlan prefer

Function:

Display the preference of the dynamic VLAN.

Parameter:

None.

Command Mode:

Admin Mode and Configuration Mode.

Usage Guide:

Display the dynamic VLAN preference.

Example:

Display current dynamic VLAN preference.

Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan

11.2.7 show mac-vlan

Command:

show mac-vlan

Function:

Display the configuration of MAC-based VLAN on the switch.

Parameter:

None.

Command Mode:

Admin Mode and other configuration Mode.

Usage Guide:

Display the configuration of MAC-based VLAN on the switch.

Example:

Display the configuration of the current MAC-based VLAN.

Switch#show mac-vlan		
MAC-Address	VLAN_ID	Priority

```
------------------          -----------     --------
00-e0-4c-77-ab-9d           2               2
00-0a-eb-26-8d-f3           2               2
00-30-4f-11-22-33                5               5
```

11.2.8 show mac-vlan interface

Command:

show mac-vlan interface

Function:

Display the ports at MAC-based VLAN.

Parameter:

None.

Command Mode:

Admin Mode and other configuration Mode.

Usage Guide:

Display the ports of enabling MAC-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example:

Display the ports of enabling MAC-based VLAN currently.

```
Switch#show mac-vlan interface
Ethernet1/1(A)          Ethernet1/2(A)
Ethernet1/3(A)          Ethernet1/4(A)
Ethernet1/5(H)          Ethernet1/6(T)
```

11.2.9 show protocol-vlan

Command:

show portocol-vlan

Function:

Display the configuration of Protocol-based VLAN on the switch.

Parameter:

None.

Command Mode:

Admin Mode and Configuration Mode

Usage Guide:

Display the configuration of Protocol-based VLAN on the switch.

Example:

Display the configuration of the current Protocol-based VLAN.

```
Switch#show protocol-vlan
Protocol_Type                          VLAN_ID          Priority
-------------------                    -------------    ---------
mode ethernetii etype 0x800                 200              4
mode ethernetii etype 0x860                 200              4
mode snap etype 0xabc                       100              5
mode llc dsap 0xac ssap 0xbd                100              5
```

11.2.10 show subnet-vlan

Command:

show subnet-vlan

Function:

Display the configuration of the IP-subnet-based VLAN on the switch.

Parameter:

None.

Command Mode:

Admin Mode and other Configuration Mode.

Usage Guide:

Display the configuration of the IP-subnet-based VLAN on the switch.

Example:

Display the configuration of the current IP-subnet-based VLAN.

```
Switch#show subnet-vlan
IP-Address              Mask                    VLAN_ID
------------------      -----------------       -------
192.168.1.165           255.255.255.0           2
202.200.121.21          255.255.0.0             2
10.0.0.1                255.248.0.0             5
```

11.2.11 show subnet-vlan interface

Command:

show subnet-vlan interface

Function:

Display the port at IP-subnet-based VLAN.

Parameter:

None.

Command Mode:

Admin Mode and other Configuration Mode.

Usage Guide:

Display the port of enabling IP-subnet-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example:

Display the port of enabling IP-subnet-based VLAN currently.

```
SwitchA#show subnet-vlan interface
Ethernet1/1(A)          Ethernet1/2(A)
Ethernet1/3(A)          Ethernet1/4(A)
Ethernet1/5(H)          Ethernet1/6(T)
```

11.2.12 subnet-vlan

Command:

subnet-vlan ip-address <ipv4-addrss> mask <subnet-mask> vlan <vlan-id> priority <priority-id>no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask>|all}

Function:

Add a correspondence between the IP subnet and the VLAN, namely add specified IP subnet into specified VLAN; the “no" form of this command deletes all/the correspondence.

Parameter:

ipv4-address is the IPv4 address shown in dotted decimal notation; the valid range of each section is 0~255; subnet-mask is the subnet mask code shown in dotted decimal notation; the valid range of each section is 0~255; priority-id is the priority applied in the VLAN tag with a valid range of 0~7; vlan-id is the VLAN ID with a valid range of 1~4094;all indicates all the subnets.

Command Mode:

Global Mode.

Default:

No IP subnet joined the VLAN by default.

Usage Guide:

This command is used for adding specified IP subnet to specified VLAN. When packet without VLAN label and from the specified IP subnet enters through the switch port, it will be matched with specified VLAN id and enters specified VLAN. These packets will always come to the same VLAN no matter through which port did they enter. This command will not interfere with VLAN labeled data packets.

Example:

Add the network equipment with IP subnet of 192.168.1.0/24 to VLAN 300.

```
SwitchA#config
```

```
SwitchA(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0
```

11.2.13 switchport mac-vlan enable

Command:

switchport mac-vlan enable

no switchport mac-vlan enable

Function:

Enable the MAC-based VLAN function on the port; the "no" form of this command will disable the MAC-based VLAN function on the port.

Parameter:

None.

Command Mode:

Port Mode.

Default:

The MAC-base VLAN function is enabled on the port by default.

Usage Guide:

After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications.

Example:

Disable the MAC-based VLAN function on port1.

Switch#config
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#no switchport mac-vlan enable

11.2.14 switchport subnet-vlan enable

Command:

switchport subnet-vlan enable

no switchport subnet-vlan enable

Function:

Enable the IP-subnet-based VLAN on the port; the "no" form of this command disables the IP-subnet-based VLAN function on the port.

Parameter:

None.

Command Mode:

Port Mode.

Default:

The IP-subnet-based VLAN is enabled on the port by default.

Usage Guide:

After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.

Example:

Disable the IP-subnet-based VLAN function on port1.

```
Switch#config
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#no switchport subnet-vlan enable
```

11.3 Commands for Voice VLAN Configuration

11.3.1 show voice-vlan

Command:

show voice-vlan

Function:

Display the configuration status of the Voice VLAN on the switch.

Parameter:

None.

Command Mode:

Admin Mode and other Configuration Mode.

Usage Guide:

Display Voice VLAN Configuration.

Example:

Display the Current Voice VLAN Configuration.

```
Switch#show voice-vlan
Voice VLAN ID:2
Ports:ethernet1/1;ethernet1/3
Voice name            MAC-Address                Mask         Priority
------------  -----   ----------------------     -----        --------
financePhone     00-e0-4c-77-ab-9d               0xff          5
manager          00-0a-eb-26-8d-f3               0xfe          6
Mr_Lee           00-30-4f-11-22-33               0x80          5
NULL             00-30-4f-11-22-33               0x0           5
```

11.3.2 switchport voice-vlan enable

Command:

switchport voice-vlan enable

no switchport voice-vlan enable

Function:

Enable the Voice VLAN function on the port; the “no” form of this command disables Voice VLAN function on the port.

Parameter:

None.

Command Mode:

Port Mode.

Default:

Voice VLAN is enabled by default.

Usage Guide:

When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user.

Example:

Disable the Voice VLAN function on port3.

Switch#config
Switch(config)#interface ethernet 1/3
Switch(Config-If-Ethernet1/3)#no switchport voice-vlan enable

11.3.3 voice-vlan

Command:

voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>]

no voice-vlan {mac <mac-address> mask <mac-mask>|name <voice-name> |all}

Function:

Specify certain voice equipment to join in Voice VLAN; the "no" form of this command will let the equipment leave the Voice VLAN.

Parameter:

Mac-address is the voice equipment MAC address, shown in ”xx-xx-xx-xx-xx-xx” format; mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0,0x80, 0x0; priority-id is the priority of the voice traffic, the valid range is 0–7; the voice-name is the name of the voice equipment, which is to facilitate the equipment management; all indicates all the MAC addresses of the voice equipments.

Command Mode:

Global Mode.

Default:

This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.

Example:

Add the 256 sets of voice equipments of the R&D department with MAC address ranging from 00-30-4f-11-22-00 to 00-30-4f-11-22-ff to the Voice VLAN.

Switch#config
Switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-30-4f-11-22-00 mask 0 priority 5 name test

11.3.4 voice-vlan vlan

Command:

voice-vlan vlan <*vlan-id*>

no voice-vlan

Function:

Configure the specified VLAN to Voice VLAN; the "**no voice-vlan**" command cancels the Voice VLAN configuration of this VLAN.

Parameter:

Vlan id is the number of the specified VLAN.

Command Mode:

Global Mode.

Default:

No Voice VLAN is configured by default.

Usage Guide:

Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN.

Example:

Set VLAN100 to Voice VLAN.

Switch#config
Switch(config)#voice-vlan vlan 100

Chapter 12 Commands for MAC Address Table Configuration

12.1 Commands for MAC Address Table Configuration

12.1.1 mac-address-table aging-time

Command:

mac-address-table aging-time <*0* | *aging-time*>

no mac-address-table aging-time

Function:

Sets the aging-time for the dynamic entries of MAC address table.

Parameter:

<aging-time> is the aging-time seconds, range form 10 to 1000000; 0 to disable aging.

Command Mode:

Global Mode.

Default:

Default aging-time is 300 seconds.

Usage Guide:

The user had better set the aging-time according to the network condition. A too small aging-time will affect the performance of the switch by causing too much broadcast, while a too large aging-time will make the unused entries stay too long in the address table.

The dynamic address does aging when the aging-time is set to 0.

Example:

Set the aging-time to 600 seconds.

```
Switch (config)#mac-address-table aging-time 600
```

12.1.2 mac-address-table static|blackhole

Command:

mac-address-table {static | blackhole} address <*mac-addr*> vlan <*vlan-id*> [interface [ethernet | portchannel] <*interface-name*>] | [source | destination | both]

no mac-address-table {static | blackhole | dynamic} [address <*mac-addr*>] [vlan <*vlan-id*>] [interface [ethernet | portchannel] <*interface-name*>]

Function:

Add or modify static address entries and filter address entries. The "**no mac-address-table {static | blackhole | dynamic} [address <*mac-addr*>] [vlan <*vlan-id*>] [interface [ethernet | portchannel] <*interface-name*>]**" command deletes the two entries.

Parameter:

static is the static entries;

blackhole is filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both. When choose the filter entries, blackhole address can't based on port, and not configure to interface;

dynamic is dynamic address entries;

<mac-addr> MAC address to be added or deleted;

<interface-name> name of the port transmitting the MAC data packet;

<vlan-id> is the vlan number.

source is based on source address filter;

destination is based on destination address filter;

both is based on source address and destination address filter, the default is both.

Command Mode:

Global Mode

Default:

When VLAN interface is configured and is up, the system will generate an static address mapping entry of which the inherent MAC address corresponds to the VLAN number.

Usage Guide:

In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.

no mac-address-table command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except for the mapping entries retained in the system default.

Example:

Port 1/1 belongs to VLAN200, and establishes address mapping with MAC address 00-30-4f-f0-00-18.

```
Switch(config)#mac-address-table static address 00-30-4f-f0-00-18 vlan 200 interface ethernet 1/1
```

12.1.3 show mac-address-table

Command:

show mac-address-table [static | blackhole | multicast | aging-time <*aging-time*> | count] [address <*mac-addr*>] [vlan <vlan-id>] [count] [interface <interface-name>]

Function:

Show the current MAC table.

Parameter:

static static entries; **blackhole** filter entries; **aging-time <*aging-time*>** address aging time; **count** entry's number, **multicast** multicast entries; ***<mac-addr>*** entry's MAC address; ***<vlan-id>*** entry's VLAN number; ***<interface-name>*** entry's interface name.

Command mode:

Admin Mode and Configuration Mode.

Default:

MAC address table is not displayed by default.

Usage guide:

This command can display various sorts of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

Example:

Display all the filter MAC address entries.

```
Switch#show mac-address-table blackhole
```

12.2 Commands for Mac Address Binding configuration

12.2.1 clear port-security dynamic

Command:

clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]

Function:

Clear the Dynamic MAC addresses of the specified port.

Command mode:

Admin Mode.

Parameter:

<mac-addr> stands MAC address; ***<interface-id>*** for specified port number.

Usage Guide:

The secure port must be locked before dynamic MAC clearing operation can be perform in specified port. If no ports and MAC are specified, then all dynamic MAC in all locked secure ports will be cleared; if only port but no MAC address is specified, then all MAC addresses in the specified port will be cleared.

Example:

Delete all dynamic MAC in port1.

```
Switch#clear port-security dynamic interface Ethernet 1/1
```

12.2.2 show port-security

Command:

show port-security

Function:

Display the secure MAC addresses of the port.

Command mode:

Admin Mode and other configuration Mode.

Default:

The switch is not display port-security configuration.

Usage Guide:

This command displays the secure port MAC address information.

Example:

```
Switch#show port-security
Security Port       MaxSecurity Addr    CurrentAddr      Security Action
                        (count)            (count)
-------------------------------------------------------------------------------------------
Ethernet1/1             1                   1            Protect
Ethernet1/3             10                  1            Protect
```

```
Ethernet1/5              1                    0              Protect
-------------------------------------------------------------------------------------------------
Max Addresses limit in System :128
Total Addresses in System :2
```

Displayed information Explanation
Security Port Is port enabled as a secure port.
MaxSecurityAddr The maximum secure MAC address number set for the security port.
CurrentAddr The current secure MAC address number of the security port.
Security Action The violation mode of the port configuration.
Total Addresses in System The current secure MAC address number of the system.
Max Addresses limit in System The maximum secure MAC address number of the system.

12.2.3 show port-security address

Command:

show port-security address [interface <*interface-id*>]

Function:

Display the secure MAC addresses of the port.

Command mode:

Admin Mode and other configuration Mode.

Parameter:

<interface-id > stands for the port to be displayed.

Usage Guide:

This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed.

Example:

```
Switch#show port-security address interface ethernet 1/3
```

```
Security Mac Address Table
------------------------------------------------------------------------------------------
Vlan       Mac Address                 Type                          Ports
 1         0000.0000.1111              SecureConfigured              Ethernet1/1
------------------------------------------------------------------------------------------
Total Addresses : 1
```

Displayed information Explanation
Vlan The VLAN ID for the secure MAC Address.
Mac Address Secure MAC address.
Type Secure MAC address type.
Ports The port that the secure MAC address belongs to.
Total Addresses Current secure MAC address number in the system.

12.2.4 show port-security interface

Command:

show port-security interface *<interface-id>*

Function:

Display the configuration of secure port.

Command mode:

Admin Mode and other configuration Mode.

Parameter:

<interface-id > stands for the port to be displayed.

Default:

Configuration of secure ports is not displayed by default.

Usage Guide:

This command displays the detailed configuration information for the secure port.

Example:

```
Switch#show port-security interface ethernet 1/1
Port Security : Enabled
Port status : Security Up
Violation mode : Protect
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Lock Timer is ShutDown
Mac-Learning function is : Opened
```

Displayed information Explanation
Port Security Is port enabled as a secure port.
Port status Port secure status.
Violation mode Violation mode set for the port.
Maximum MAC Addresses The maximum secure MAC address number set for the port.
Total MAC Addresses Current secure MAC address number for the port.
Configured MAC Addresses Current secure static MAC address number for the port.
Lock Timer Whether locking timer (timer timeout) is enabled for the port.
Mac-Learning function Is the MAC address learning function enabled.

12.2.5 switchport port-security

Command:

switchport port security

no switchport port security

Function:

Enable MAC address binding function for the port; the "**no switchport port-security**" command disables the MAC address binding function for the port.

Command mode:

Port Mode.

Default:

MAC address binding is not enabled by default.

Usage Guide:

The MAC address binding function and Port Aggregation functions are mutually exclusive. Therefore, if MAC binding function for a port is to be enabled, the Port Aggregation functions must be disabled, and the port enabling MAC address binding must not be a Trunk port.

Example:

Enable MAC address binding function for port 1and.

```
Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)# switchport port security
```

12.2.6 switchport port-security convert

Command:

switchport port-security convert

Function:

Converts dynamic secure MAC addresses learned by the port to static secure MAC addresses, and disables the MAC address learning function for the port.

Command mode:

Port Mode.

Usage Guide:

The port dynamic MAC convert command can only be executed after the secure port is locked. After this command has been executed, dynamic secure MAC addresses learned by the port will be converted to static secure MAC addresses. The command does not reserve configuration.

Example:

Converting MAC addresses in port 1 to static secure MAC addresses.

```
Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)# switchport port-security convert
```

12.2.7 switchport port-security lock

Command:

switchport port-security lock

no switchport port-security lock

Function:

Lock the port. After the port is locked, the MAC-address learning function will be shut down; the no operation of this command will reset the MAC-address learning function.

Command Mode:

Port Configuration Mode.

Default:

Ports are unlocked.

Usage Guide:

Ports can only be locked after the MAC-address binding function is enabled. When a port becomes locked, its MAC learning function will be disabled.

Examples:

Lock port 1.

```
Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)#switchport port-security lock
```

12.2.8 switchport port-security mac-address

Command:

switchport port-security mac-address <*mac-address*>

no switchport port-security mac-address <*mac-address*>

Function:

Add a static secure MAC address; the "**no switchport port-security mac-address**" command deletes a static secure MAC address.

Command mode:

Port Mode.

Parameters:

<mac-address> stands for the MAC address to be added or deleted.

Usage Guide:

The MAC address binding function must be enabled before static secure MAC address can be added.

Example:

Adding MAC 00-30-4f-FE-2E-D3 to port1.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security mac-address 00-30-4f-FE-2E-D3
```

12.2.9 switchport port-security maximum

Command:

switchport port-security maximum <*value*>

no switchport port-security maximum

Function:

Sets the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the maximum secure address number of 1.

Command mode:

Port Mode.

Parameter:

< *value*> is the up limit for static secure MAC address, the valid range is 1 to 128.

Default:

The default maximum port secure MAC address number is 1.

Usage Guide:

The MAC address binding function must be enabled before maximum secure MAC address number can be set. If secure static MAC address number of the port is larger than the maximum secure MAC address number set, the setting fails; extra secure static MAC addresses must be deleted, so that the secure static MAC address number is no larger than the maximum secure MAC address number for the setting to be successful.

Example:

Set the maximum secure MAC address number for port 1.

Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)# switchport port-security maximum 4

12.2.10 switchport port-security timeout

Command:

switchport port-security timeout <*value*>

no switchport port-security timeout

Function:

Set the timer for port locking; the "**no switchport port-security timeout**" command restores the default setting.

Parameter:

< *value*> is the timeout value, the valid range is 0 to 300s.

Command mode:

Port Mode.

Default:

Port locking timer is not enabled by default.

Usage Guide:

The port locking timer function is a dynamic MAC address locking function. MAC address locking and conversion of dynamic MAC entries to secure address entries will be performed on locking timer timeout. The MAC address binding function must be enabled prior to running this command.

Example:

Set port1 locking timer to 30 seconds.

Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)# switchport port-security timeout 30

12.2.11 switchport port-security violation

Command:

switchport port-security violation {protect | shutdown}

no switchport port-security violation

Function:

Configure the port violation mode. The "**no switchport port-security violation**" restore the violation mode to protect.

Command Mode:

Port mode.

Parameter:

protect refers to protect mode; **shutdown** refers to shutdown mode.

Default:

The port violation mode is **protect** by default.

Usage Guide:

The port violation mode configuration is only available after the MAC address binding function is enabled. when the port secure MAC address exceeds the security MAC limit, if the violation mode is protect, the port only disable the dynamic MAC address learning function; while the port will be shut if at shutdown mode. Users can manually open the port with no shutdown command.

Example：

Set the violation mode of port 1 to shutdown.

Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)# switchport port-security violation shutdown

Chapter 13 ommands for MSTP

13.1 Commands for MSTP

13.1.1 abort

Command:

abort

Function:

Abort the current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode:

MSTP Region Mode.

Usage Guide:

This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid.

Example:

Quit MSTP region mode without saving the current configuration.

```
Switch(Config-Mstp-Region)#abort

Switch(config)#
```

13.1.2 exit

Command:

exit

Function:

Save current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode:

MSTP Region Mode

Usage Guide:

This command is to quit MSTP region mode with saving the current configuration.

Example:

Quit MSTP region mode with saving the current configuration.

```
Switch(Config-Mstp-Region)#exit

Switch(config)#
```

13.1.3 instance vlan

Command:

instance <*instance-id*> vlan <*vlan-list*>

no instance <*instance-id*> [vlan <*vlan-list*>]

Function:

In MSTP region mode, create the instance and set the mappings between VLANs and instances; the command "**no instance <*instance-id*> [vlan <*vlan-list*>]**" removes the specified instance and the specified mappings between the VLANs and instances.

Parameter:

Normally, ***<instance-id>*** sets the instance number. The valid range is from 0 to 48; In the command "**no instance <*instance-id*> [vlan <*vlan-list*>]**", ***<instance-id>*** sets the instance number. The valid number is from 0 to 48. ***<vlan-list>*** sets consecutive or non-consecutive VLAN numbers. "-" refers to consecutive numbers, and ";" refers to non-consecutive numbers.

Command mode:

MSTP Region Mode

Default:

Before creating any Instances, there is only the instance 0, and VLAN 1~4094 all belong to the instance 0.

Usage Guide:

This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 48 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 48.

Example:

Map VLAN1-10 and VLAN 100-110 to Instance 1.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110
```

13.1.4 name

Command:

name <*name*>

no name

Function:

In MSTP region mode, set MSTP region name; the "**no name**" command restores the default setting.

Parameter:

<name> is the MSTP region name. The length of the name should be less than 32 characters.

Command mode:

MSTP Region Mode

Default:

Default MSTP region name is the MAC address of this bridge.

Usage Guide:

This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.

Example:

Set MSTP region name to mstp-test.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#description mstp-test
```

13.1.5 revision-level

Command:

revision-level *<level>*

no revision-level

Function:

In MSTP region mode, this command is to set revision level for MSTP configuration; the command "**no revision-level**" restores the default setting to 0.

Parameter:

<level> is revision level. The valid range is from 0 to 65535.

Command mode:

MSTP Region Mode

Default:

The default revision level is 0.

Usage Guide:

This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.

Example:

Set revision level to 2000.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)# revision-level 2000
```

13.1.6 spanning-tree

Command:

spanning-tree

no spanning-tree

Function:

Enable MSTP in global mode and in Port Mode; The command "**no spanning-tree**" is to disable MSTP.

Command mode:

Global Mode and Port Mode

Default:

MSTP is not enabled by default.

Usage Guide:

If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly.

Example:

Enable the MSTP in global mode, and disable the MSTP in the interface1/2.

```
Switch(config)#spanning-tree
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#no spanning-tree
```

13.1.7 spanning-tree forward-time

Command:

spanning-tree forward-time <*time*>

no spanning-tree forward-time

Function:

Set the switch forward delay time; the command "**no spanning-tree forward-time**" restores the default setting.

Parameter:

<time> is forward delay time in seconds. The valid range is from 4 to 30.

Command mode:

Global Mode

Default:

The forward delay time is 15 seconds by default.

Usage Guide:

When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example:

In global mode, set MSTP forward delay time to 20 seconds.

```
Switch(config)#spanning-tree forward-time 20
```

13.1.8 spanning-tree hello-time

Command:

spanning-tree hello-time <*time*>

no spanning-tree hello-time

Function:

Set switch Hello time; The command "**no spanning-tree hello-time**" restores the default setting.

Parameter:

<time> is Hello time in seconds. The valid range is from 1 to 10.

Command mode:

Global Mode

Default:

Hello Time is 2 seconds by default.

Usage Guide:

Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example:

Set MSTP hello time to 5 seconds in global mode.

```
Switch(config)#spanning-tree hello-time 5
```

13.1.9 spanning-tree link-type p2p

Command:

spanning-tree link-type p2p {auto | force-true | force-false}

no spanning-tree link-type

Function:

Set the link type of the current port; the command "**no spanning-tree link-type**" restores link type to auto-negotiation.

Parameter:

auto sets auto-negotiation, **force-true** forces the link as point-to-point type, **force-false** forces the link as non point-to-point type.

Command mode:

Port Mode

Default:

The link type is auto by default, The MSTP detects the link type automatically.

Usage Guide:

When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.

Example:

Force the port 1/7-8 as point-to-point type.

```
Switch(config)#interface ethernet 1/7-8
Switch(Config-Port-Range)#spanning-tree link-type p2p force-true
```

13.1.10 spanning-tree maxage

Command:

spanning-tree maxage <*time*>

no spanning-tree maxage

Function:

Set the max aging time for BPDU; the command "**no spanning-tree maxage**" restores the default setting.

Parameter:

<time> is max aging time in seconds. The valid range is from 6 to 40.

Command mode:

Global Mode

Default:

The max age is 20 seconds by default.

Usage Guide:

The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example:

In global mode, set max age time to 25 seconds.

```
Switch(config)#spanning-tree maxage 25
```

13.1.11 spanning-tree max-hop

Command:

spanning-tree max-hop <*hop-count*>

no spanning-tree max-hop

Function:

Set maximum hops of BPDU in the MSTP region; the command "**no spanning-tree max-hop**" restores the default setting.

Parameter:

<hop-count> sets maximum hops. The valid range is from 1 to 40.

Command mode:

Global Mode

Default:

The max hop is 20 by default.

Usage Guide:

The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.

Example:

Set max hop to 32.

```
Switch(config)#spanning-tree max-hop 32
```

13.1.12 spanning-tree mcheck

Command:

spanning-tree mcheck

Function:

Force the port to run in the MSTP mode.

Command mode:

Port Mode

Default:

The port is in the MSTP mode by default.

Usage Guide:

If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.

This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.

Example:

Force the port 1/2 to run in the MSTP mode.

```
Switch(Config-If-Ethernet1/2)#spanning-tree mcheck
```

13.1.13 spanning-tree mode

Command:

spanning-tree mode {mstp | stp | rstp}

no spanning-tree mode

Function:

Set the spanning-tree mode in the switch; The command "**no spanning-tree mode**" restores the default setting.

Parameter:

mstp sets the switch in IEEE802.1s MSTP mode; **stp** sets the switch in IEEE802.1D STP mode; **rstp** sets the switch in IEEE802.1D RSTP mode.

Command mode:

Global Mode

Default:

The switch is in the MSTP mode by default.

Usage Guide:

When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.

Example:

Set the switch in the STP mode.

```
Switch(config)#spanning-tree mode stp
```

13.1.14 spanning-tree mst configuration

Command:

spanning-tree mst configuration

no spanning-tree mst configuration

Function:

Enter the MSTP mode. Under the MSTP mode, the MSTP attributes can be set. The command "**no spanning-tree mst configuration**" restores the attributes of the MSTP to their default values.

Command mode:

Global Mode

Default:

The default values of the attributes of the MSTP region are listed as below:

Attribute of MSTP Default Value
Instance There is only the instance 0. All the VLANs (1~4094) are mapped to the instance 0.
Name MAC address of the bridge
Revision 0

Usage Guide:

Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.

Example:

Enter MSTP region mode.

Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#

13.1.15 spanning-tree mst cost

Command:

spanning-tree mst <*instance-id*> cost <*cost*>

no spanning-tree mst <instance-id> cost

Function:

Sets path cost of the current port in the specified instance; the command "**no spanning-tree mst <instance-id> cost**" restores the default setting.

Parameter:

<instance-id> sets the instance ID. The valid range is from 0 to 48. ***<cost>*** sets path cost. The valid range is from 1 to 200,000,000.

Command mode:

Port Mode

Default:

By default, the port cost is relevant to the port bandwidth.

Port Type Default Path Cost Suggested Range
10Mbps 2000000 2000000~20000000
100Mbps 200000 200000~2000000
1Gbps 20000 20000~200000
10Gbps 2000 2000~20000

For the aggregation ports, the default costs are as below:

Port Type Allowed Number Of Aggregation Ports Default Port Cost
10Mbps N 2000000/N
100Mbps N 200000/N
1Gbps N 20000/N
10Gbps N 2000/N

Usage Guide:

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example:

On the port1/2, set the MSTP port cost in the instance 2 to 3000000.

```
Switch(Config-If-Ethernet1/2)#spanning-tree mst 2 cost 3000000
```

13.1.16 spanning-tree mst port-priority

Command:

spanning-tree mst <*instance-id*> port-priority <*port-priority*>

no spanning-tree mst <*instance-id*> port-priority

Function:

Set the current port priority for the specified instance; the command "**no spanning-tree mst <*instance-id*> port-priority**" restores the default setting.

Parameter:

<instance-id> sets the instance ID. The valid range is from 0 to 48; ***<port-priority>*** sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32…240.

Command mode:

Port Mode

Default:

The default port priority is 128.

Usage Guide:

By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Example:

Set the port priority as 32 on the port 1/2 for the instance 1.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree mst 1 port-priority 32
```

13.1.17 spanning-tree mst priority

Command:

spanning-tree mst <*instance-id*> priority <*bridge-priority*>

no spanning-tree mst <*instance-id*> priority

Function:

Set the bridge priority for the specified instance; the command "**no spanning-tree mst <*instance-id*> priority**" restores the default setting.

Parameter:

<instance-id> sets instance ID. The valid range is from 0 to 48; ***<bridge-priority>*** sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192…61440.

Command mode:

Global Mode

Default:

The default bridge priority is 32768.

Usage Guide:

By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.

Example:

Set the priority for Instance 2 to 4096.

```
Switch(config)#spanning-tree mst 2 priority 4096
```

13.1.18 spanning-tree mst rootguard

Command:

spanning-tree [mst <*instance-id*>] rootguard

no spanning-tree [mst <*instance-id*>] rootguard

Function:

Enable the rootguard function for specified instance, the rootguard function forbid the port to be MSTP root port. "**no spanning-tree mst <*instance-id*> rootguard**" disable the rootguard function.

Parameter:

<instance-id>：MSTP instance ID.

Command mode:

Port Mode.

Default:

Disable rootguard function.

Usage Guide:

The command is used in Port Mode, if the port is configured to be a rootguand port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked).If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.

Example:

Enable rootguard function for port 1/2 in instance 0.

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree mst 0 rootguard
Switch(Config-If-Ethernet1/2)#

13.1.19 spanning-tree portfast

Command:

spanning-tree portfast [bpdufilter | bpduguard]

no spanning-tree portfast

Function:

Set the current port as boundary port, and BPDU filter、BPDU guard as specified mode or default mode ; the command "**no spanning-tree portfast**" sets the current port as non-boundary port.

Parameter:

bpdufilter: configure the border port mode as BPDU filter;

bpduguard: configure the border port mode as BPDU guard.

Command mode:

Port Mode

Default:

All the ports are non-boundary ports by default when enabling MSTP.

Usage Guide:

When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.

Example:

Configure the border port mode as BPDU filter.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree portfast bpdufilter
Switch(Config-If-Ethernet1/2)#
```

13.1.20 spanning-tree priority

Command:

spanning-tree priority <*bridge-priority*>

no spanning-tree priority

Function:

Configure the spanning-tree priority; the "**no spanning-tree priority**" command restores the default priority.

Parameter:

<bridge-priority> is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192… 61440.

Command Mode:

Global Mode.

Default:

Priority is 32768.

Usage Guide:

The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.

Example:

Configure the priority is 4096.

```
Switch(config)#spanning-tree priority 4096
```

13.1.21 spanning-tree format

Command:

spanning-tree format {standard | privacy | auto}

no spanning-tree format

Function:

Configure the format of the port packet so to be interactive with products of other companies. The no command restores the default format.

Parameter:

standard：The packet format provided by IEEE

privacy：Privacy packet format, which is compatible with CISCO equipments.

auto：Auto identified packet format, which is determined by checking the format of the received packets.

Default:

Auto Packet Format.

Command Mode:

Port Mode

Usage Guide:

As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies. The packet format will be privacy format before receiving the partner packet when configured to AUTO.

When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits.

When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.

Example:

Configure port message format as the message format of IEEE.

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree format standard
Switch(Config-If-Ethernet1/2)#

13.1.22 spanning-tree digest-snooping

Command:

spanning-tree digest-snooping

no spanning-tree digest-snooping

Function:

Configure the port to use the authentication string of partner port; the command "**no spanning-tree digest-snooping**" restores to use the port generated authentication string.

Parameter:

None

Command mode:

Port Mode

Default:

Don't use the authentication string of partner port.

Usage Guide:

According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, intstance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufactories equipment.

Note: Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.

Example:

Configure the authentication string of partner port.

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree digest-snooping
Switch(Config-If-Ethernet1/2)#

13.1.23 spanning-tree tcflush (Global mode)

Command:

spanning-tree tcflush {enable| disable| protect}

no spanning-tree tcflush

Function:

Configure the spanning-tree flush mode once the topology changes. "no spanning-tree tcflush" restores to default setting.

Parameter:

enable: The spanning-tree flush once the topology changes.

disable: The spanning tree don't flush when the topology changes.

protect: the spanning-tree flush not more than one time every ten seconds.

Command mode:

Global mode

Default:

Enable

Usage Guide:

According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note: For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example:

Configure the spanning-tree flush mode once the topology changes is not flush to TC.

```
Switch(config)#spanning-tree tcflush disable

Switch(config)#
```

13.1.24 spanning-tree tcflush (Port mode)

Command:

spanning-tree tcflush {enable| disable| protect}

no spanning-tree tcflush

Function:

Configure the spanning-tree flush mode for port once the topology changes. “no spanning-tree tcflush” restores to default setting.

Parameter:

enable: The spanning-tree flush once the topology changes.

disable: The spanning tree don’t flush when the topology changes.

protect: the spanning-tree flush not more than one time every ten seconds.

Command mode:

Port Mode

Default:

Global configuration

Usage Guide:

According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note: For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example:

Configure the spanning-tree flush mode once the topology change is not flush to TC.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#spanning-tree tcflush disable
Switch(Config-If-Ethernet1/2)#
```

13.2 Commands for Monitor and Debug

13.2.1 show spanning-tree

Command:

show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]

Function:

Display the MSTP Information.

Parameter:

<interface-list> sets interface list; ***<instance-id>*** sets the instance ID. The valid range is from 0 to 48; **detail** sets the detailed spanning-tree information.

Command mode:

Admin and Configuration Mode

Usage Guide:

This command can display the MSTP information of the instances in the current bridge.

Example:

Display the bridge MSTP.

```
Switch#sh spanning-tree

                    -- MSTP Bridge Config Info --

Standard        :   IEEE 802.1s
Bridge MAC      :   00: 30: 4f: 01: 0e: 30
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3

############################ Instance 0 ############################
Self Bridge Id     : 32768 -   00: 30: 4f: 01: 0e: 30
Root Id               : 16384.00: 30: 4f: 01: 0f: 52
Ext.RootPathCost : 200000
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID        : 128.1
Current port list in Instance 0:
Ethernet1/1 Ethernet1/2 (Total 2)
```

```
 PortName        ID        ExtRPC     IntRPC   State Role       DsgBridge       DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
 Ethernet1/1   128.001            0          0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet1/2   128.002            0          0 BLK ALTR 16384.00030f010f52 128.011

############################## Instance 3 ##############################
Self Bridge Id    : 0.00: 30: 4f: 01: 0e: 30
Region Root Id    : this switch
Int.RootPathCost : 0
Root Port ID      : 0
Current port list in Instance 3:
Ethernet1/1 Ethernet1/2 (Total 2)

   PortName        ID      IntRPC     State Role       DsgBridge       DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1   128.001            0 FWD MSTR       0.00030f010e30 128.001
 Ethernet1/2   128.002            0 BLK ALTR       0.00030f010e30 128.002

############################## Instance 4 ##############################
Self Bridge Id    : 32768.00: 30: 4f: 01: 0e: 30
Region Root Id    : this switch
Int.RootPathCost : 0
Root Port ID      : 0
Current port list in Instance 4:
Ethernet1/1 Ethernet1/2 (Total 2)

   PortName        ID      IntRPC     State Role       DsgBridge       DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1 128.001            0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet1/2 128.002            0 BLK ALTR 32768.00030f010e30 128.002
```

Displayed Information Description
Bridge Information
Standard STP version
Bridge MAC Bridge MAC address

Bridge Times Max Age, Hello Time and Forward Delay of the bridge
Force Version Version of STP
Instance Information
Self Bridge Id The priority and the MAC address of the current bridge for the current instance
Root Id The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost Total cost from the current bridge to the root of the entire network
Int.RootPathCost Cost from the current bridge to the region root of the current instance
Root Port ID Root port of the current instance on the current bridge
MSTP Port List Of The Current Instance
PortName Port name
ID Port priority and port index
ExtRPC Port cost to the root of the entire network
IntRPC

Cost from the current port to the region root of the current instance
State Port status of the current instance
Role Port role of the current instance
DsgBridge Upward designated bridge of the current port in the current instance
DsgPort Upward designated port of the current port in the current instance

13.2.2 show spanning-tree mst config

Command:

show spanning-tree mst config

Function:

Display the configuration of the MSTP in the Admin mode.

Command mode:

Admin Mode

Usage Guide:

In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

Example:

Display the configuration of the MSTP on the switch.

```
Switch#show spanning-tree mst config

Name          switch
Revision      0
Instance      Vlans Mapped
------------------------------------
00            1-29, 31-39, 41-4094
03              30
04            40
------------------------------------
```

13.2.3 show mst-pending

Command:

show mst-pending

Function:

In the MSTP region mode, display the configuration of the current MSTP region.

Command mode:

Admin Mode

Usage Guide:

In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.

Note: Before quitting the MSTP region mode, the displayed parameters may not be effective.

Example:

Display the configuration of the current MSTP region.

```
Switch(config)#spanning-tree mst configuration
```

```
Switch(Config-Mstp-Region)#show mst-pending
Name          switch
Revision      0
Instance      Vlans Mapped
---------------------------------
00            1-29, 31-39, 41-4093
03            30
04            40
05            4094
---------------------------------
```

```
Switch(Config-Mstp-Region)#
```

13.2.4 debug spanning-tree

Command:

debug spanning-tree

no debug spanning-tree

Function:

Enable the MSTP debugging information; the command "**no debug spanning-tree**" disables the MSTP debugging information.

Command mode:

Admin Mode

Usage Guide:

This command is the general switch for all the MSTP debugging. Users should enable the detailed debugging information, then they can use this command to display the relevant debugging information. In general, this command is used by skilled technicians.

Example:

Enable to receive the debugging information of BPDU messages on the port1/1.

Switch#debug spanning-tree
Switch#debug spanning-tree bpdu rx interface e1/1

Chapter 14 Commands for QoS and PBR

14.1 class

Command:

class <*class-map-name*>

no class <*class-map-name*>

Function:

Associates a class to a policy map and enters the policy class map mode; the "**no class <*class-map-name*>**" command deletes the specified class.

Parameters:

< *class-map-name*> is the class map name used by the class.

Default:

No policy class is configured by default.

Command mode:

Policy map configuration Mode

Usage Guide:

Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and policy configuration can be performed on packet traffic classified by class map.

Example:

Entering a policy class mode.

Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit

14.2 class-map

Command:

class-map <*class-map-name*>

no class-map <*class-map-name*>

Function:

Creates a class map and enters class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.

Parameters:

<class-map-name> is the class map name.

Default:

No class map is configured by default.

Command mode:

Global Mode

Usage Guide:

Example:

Creating and then deleting a class map named “c1”.

Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1

14.3 match

Command:

match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*> | ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*> | ipv6 flowlabel <*flowlabel-list*> | vlan <*vlan-list*> | cos<*cost-list*>}

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos }

Function:

Configure the match standard of the class map; the “no” form of this command deletes the specified match standard.

Parameter:

access-group <*acl-index-or-name*> match specified IP ACL or MAC ACL, the parameters are the number or name of the ACL;

ip dscp <*dscp-list*> and **ipv6 dscp <*dscp-list*>** match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values;

ip precedence <*ip-precedence-list*> match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;

ipv6 access-group <*acl-index-or-name*> match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;

ipv6 flowlabel <*flowlabel-list*> match specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0~1048575;

vlan <*vlan-list*> match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs.

<*cost-list*> match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS.

Default:

No match standard by default

Command Mode:

Class-map Mode

Usage Guide:

Only one match standard can be configured in a class map. When configuring match the ACL, only the permit rule is available in the ACL.

Example:

Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0.

Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0
Switch(Config-ClassMap-c1)#exit

14.4 mls qos

Command:

mls qos

no mls qos

Function:

Enables QoS in Global Mode; the "**no mls qos**" command disables the global QoS.

Parameter:

None.

Command mode:

Global Mode.

Default:

QoS is disabled by default.

Usage Guide:

QoS provides 8 queues to handle traffics of 8 priorities. The rule is taking effect by default when startup, message will rewrite cos field according to cos-dscp-cos, dscp-mutation rewrite dscp value according to cos-dscp. Ingress cos value is the port default cos.

Example:

Enabling and then disabling the QoS function.

Switch(config)#mls qos
Switch(config)#no mls qos

14.5 mls qos cos

Command:

mls qos cos {<*default-cos*> }

no mls qos cos

Function:

Configures the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.

Parameters:

<default-cos> is the default CoS value for the port, the valid range is 0 to 7.

Default:

The default CoS value is 0.

Command mode:

Interface Configuration Mode.

Usage Guide:

Configure the default CoS value for switch port. The message ingress cos from this port are default value whether the message have tag. If the message have no tag, the message cos value for tag is enactmented.

Example:

Setting the default CoS value of ethernet port 1/1 to 5, i.e., packets coming in through this port will be assigned a default CoS value of 5 if no CoS value present.

```
Switch(config)#interface ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#mls qos cos 5
```

14.6 mls qos aggregate-policy

Command:

Single Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) | exceed-action (drop | policed-dscp-transmit | transmit) })

no mls qos aggregate-policy

Dual Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> |) <maximum_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) exceed-action (drop | policed-dscp-transmit | transmit) | violate-action (drop | policed-dscp-transmit | transmit)})

no mls qos aggregate-policy

Function:

Analyze the working mode of the token bucket, whether it is single rate singe bucket, singe rate dual bucket or dual rate dual bucket. The no operation will delete the mode configuration.

Parameters:

policer_name：the name of aggregation policer;

bits_per_second：the committed information rate - CIR , in Kbps, ranging from 1 to 10000000;

normal_burst_bytes：the committed burst size – CBS, in kb, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;

pir peak_rate_bps：the peak information rate, in kbps, ranging from 1to 10000000. Without configuring PIR, the Police works in the single rate dual bucket mode; otherwise in the dual rate dual bucket mode. Notice: this configuration only exist in the dual bucket mode. Notice: this configuration only exists in dual bucket mode;

maximum_burst_bytes：the peak burst size, in kb, ranging from 1to 10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by

the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode;

conform-action：the actions to take when the CIR is not exceeded, which means the messages are green, including drop;

set-dscp-transmit：change dscp (ranging from 0 to 63), set-prec-transmit: change TOS (ranging from 0 to 1), transmit: messages will pass without any action;

qate-action：the actions to take when the PIR is exceeded, which means the messages are red, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action. Notice: this action only exists in dual bucket mode.

Default:

No aggregation Policer is defined by default; the default action of conform-action is transmit, while that of exceed-action and violate-action both is drop.

Command mode:

Global Mode

Usage Guide:

The CLI can support both singe bucket and dual bucket configuration, and determine which one to select by checking whether violate-action is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single rate single bucket; if only PBS is configured, the mode is single rate dual bucket; if PIR and PBS are configured, the mode is dual rate dual bucket.

Example:

Set the single bucket mode, CIR is 1000, CBS is 1000. The action to take is drop, when the CIR is not exceeded, which means the messages are green; the action is policed-dscp-transmit (change the DSCP value and then transmit the messages) when the CIR is exceeded but PIR isn't, which means the messages are yellow.

```
Switch(config)#mls qos aggregate-policy color 1000 1000 conform-action drop exceed-action policed-dscp-transmit
```

14.7 mls qos trust

Command:

mls qos trust {cos [pass-through-cos] [pass-through-dscp]|dscp [pass-through-cos] [pass-through-dscp]| ip-precedence [pass-through-cos] [pass-through-dscp] |port priority <cos> [pass-through-cos] [pass-through-dscp]}

no mls qos trust

Function:

Configures port trust; the "**no mls qos trust**" command disables the current trust status of the port.

Parameters:

cos configures the port to trust CoS value; **cos pass-through-dscp** configures the port to trust CoS value but does not change packet DSCP value; **dscp** configures the port to trust DSCP value; **dscp pass-through-cos** configures the port to trust DSCP value, but does not change packet CoS value; **ip-precedence** configures the port to trust IP precedence; **ip-precedence pass-through-cos** configures the port to trust IP precedence, but does not change packet CoS value.

port priority <*cos*> assigns a priority to the physical port, **cos** is the priority to be assigned. Priority of all incoming packets through the port will be set to this cos value. This is irrelevant to the priority of the packet itself, no modification is done to the packets.

Default:

No trust.

Command mode:

Interface Configuration Mode.

Usage Guide:

trust cos mode: can setting the message cos field based cos-dscp-cos, setting the message dscp value based cos-dscp, dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust dscp mode: can setting the message cos field based dscp-cos, setting the message dscp value based dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust ip-precedence mode: can setting the message cos field based ip-precedence-dscp-cos, setting the message dscp value based ip-precedence-dscp，dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust port mode: can setting the message cos field based cos-dscp-cos, setting the message dscp value based cos-dscp ，dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

Example:

Configuring ethernet port 1/1 to trust CoS value, i.e., classifying the packets according to CoS value.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos trust cos
```

14.7.1 mls qos dscp-mutation

Command:

mls qos dscp-mutation <*dscp-mutation-name*>

no mls qos dscp-mutation <*dscp-mutation-name*>

Function:

Applies DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

Parameters:

<dscp-mutation-name> is the name of DSCP mutation mapping.

Default:

There is no policy by default.

Command mode:

Interface Configuration Mode.

Usage Guide:

For configuration of DSCP mutation mapping on the port to take effect, the port can configure no trust status or configure any trust status, but can not be used with pass-through-dscp command in trust status. DSCP mutation mapping is good for this port.

Example:

Configuring Ethernet port 1/1 to trust DSCP, using DSCP mutation mapping of mu1.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos trust dscp pass-through-cos
Switch(Config-If-Ethernet1/1)#mls qos dscp-mutation mu1
```

14.7.2 mls qos map

Command:

mls qos map (cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |*ip-prec-dscp* <dscp1...dscp8> | policed-dscp *(normal-burst* | max-burst) <dscp-list> to <mark-down-dscp>)

no mls qos *map* (cos-dscp | dscp-cos | dscp-mutation <dscp-mutation-name> | ip-prec-dscp | policed-dscp (normal-burst | max-burst))

Function:

Support the configuration of all actions in dual rate dual bucket mode. Sets class of service (CoS)-to-Differentiated Services Code Point (DSCP) mapping, DSCP to CoS mapping, DSCP to DSCP mutation mapping, IP precedence to DSCP and policed DSCP mapping; the exceed-action and violate-action use different policied-dscp map tables. The no command restores the default mapping.

Parameters:

cos-dscp <*dscp1...dscp8*> defines the mapping from CoS value to DSCP-inside, **<*dscp1...dscp8*>** are the 8 DSCP-inside value corresponding to the 0 to 7 CoS value, each DSCP-inside value is delimited with space, ranging from 0 to 63; **dscp-cos <*dscp-list*> to <*cos*>** defines the mapping from DSCP-inside to CoS value, **<*dscp-list*>** is a list of DSCP value consisting of up to 8 DSCP-inside values, **<*cos*>** are the CoS values corresponding to the DSCP values in the list; **dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** defines the mapping from DSCP to DSCP mutation, **<*dscp-mutation-name*>** is the name for mutation mapping, **<*in-dscp*>** stand for incoming DSCP-inside values, up to 8 values are supported, each DSCP-inside value is delimited with space, ranging from 0 to 63, **<*out-dscp*>** is the sole outgoing DSCP value, the 8 values defined in incoming DSCP will be converted to outgoing DSCP values; **ip-prec-dscp <*dscp1...dscp8*>** defines the conversion from IP precedence to DSCP-inside value, **<*dscp1...dscp8*>** are 8 DSCP-inside values corresponding to IP precedence 0 to 7, each DSCP value is delimited with space, ranging from 0 to 63; **policed-dscp <dscp-list> to <mark-down-dscp>** defines DSCP mark down mapping, where **<dscp-list>** is a list of DSCP values containing up to 8 DSCP values, **<mark-down-dscp>** are DSCP value after mark down.

Default:

Default mapping values are:

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation and policed-dscp are not configured by default

Command mode:

Global Mode

Usage Guide:

The dscp which in cos-dscp, dscp-cos, ip-prec-dscp, dscp-mutation fingers dscp-inside value. Because of the dscp-inside value have 64 and that the chip priority-inside only 8, the dscp-cos mapping need 8 continuum dscp-inside mapping to the same cos, in other words, dscp 0-7 mapping the same cos value.

Example:

1. Setting the CoS-to-DSCP mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7.

```
Switch(config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7
```

2. Mapping DSCP 1, 2 to COS 7.

```
Switch(config)#mls qos map dscp-cos 1 2 to 7
```

14.7.3 policy

Command:

Single Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit *<ip_precedence_value>* | transmit) | exceed-action (drop | policed-dscp-transmit | transmit) })

no policy *<bits_per_second>* *<normal_burst_bytes>* ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) | exceed-action (drop | policed-dscp-transmit | transmit)})

Dual Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> |) <maximum_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit *<ip_precedence_value>* | transmit) exceed-action (drop | policed-dscp-transmit | transmit) | violate-action (drop | policed-dscp-transmit | transmit)})

no policy <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps>) <maximum_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) exceed-action (drop | policed-dscp-transmit | transmit) | violate-action (drop | policed-dscp-transmit | transmit)})

Function:

The non-aggregation policer command supporting three colors. Determine whether the working mode of token bucket is singe rage single bucket, single rate single bucket, single rate dual bucket

or dual rate dual bucket, by analyzing the parameters. The no command will delete the mode configuration.

Parameters:

bits_per_second： the committed information rate - CIR , in Kbps, ranging from 1 to 10000000.

normal_burst_bytes：the committed burst size – CBS, in kb, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt.

maximum_burst_bytes：the peak burst size, in kb, ranging from 1 to 10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode.

pir peak_rate_bps :the peak burst size, in kb, ranging from 1 to 10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode.

conform-action：the actions to take when the CIR is not exceeded, which means the messages are green, including drop, set-dscp-transmit: change dscp (ranging from 0 to 63), set-prec-transmit: change TOS (ranging from 0 to 1), transmit: messages will pass without any action.

exceed-action：the actions to take when the CIR is exceeded but PIR isn't, which means the messages are yellow, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action.

violate-action：the actions to take when the PIR is exceeded, which means the messages are red, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action. Notice: this action only exists in dual bucket mode.

Default:

No aggregation Policer is defined by default; the default action of conform-action is transmit, while that of exceed-action and violate-action both is drop. show running-config won't display the default configurations.

Command mode:

Policy class map configuration Mode

Usage Guide:

The CLI can support both singe bucket and dual bucket configuration, and determine which one to select by checking whether violate-action is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single rate single bucket; if only PBS is configured, the mode is single rate dual bucket; if PIR and PBS are configured, the mode is dual rate dual bucket.

Example:

In the policy class table configuration mode, set the CIR as 1000, CBS as 2000 and the action when CIR is not exceeded as transmitting the messages after changing DSCP to 23, and the action triggered by exceeding CIR as transmit without changing the messages.

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
```

Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy 1000 2000 conform-action set-dscp-transmit 23 exceed-action transmit

14.7.4 policy aggregate

Command:

policy aggregate *<aggregate-policy-name>*

no policy aggregate *<aggregate-policy-name>*

Function:

Police Map reference aggregate policy, applies a policy set to classified traffic; the "**no policy aggregate *<aggregate-policy-name>***" command deletes the specified policy set.

Parameters:

<aggregate-policy-name> is the policy set name.

Default:

No policy set is configured by default.

Command mode:

Policy class map configuration Mode

Usage Guide:

The same policy set can be referred to by different policy class maps.

Example:

Create class-map, the match rule is the cos value is 0; policy-map is 1, enter the policy map mode, set the Policy and choose the color policy for the current list.

Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy aggregate color

14.7.5 policy-map

Command:

policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Function:

Creates a policy map and enters the policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.

Parameters:

< *policy-map-name*> is the policy map name.

Default:

No policy map is configured by default.

Command mode:

Global Mode

Usage Guide:

PBR classification matching and marking next hop operations can be done in the policy map configuration mode.

Example:

Creating and deleting a policy map named "p1".

Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#exit
Switch(config)#no policy-map p1

14.8 priority-queue out

Command:

priority-queue out

no priority-queue out

Function:

Configure the dequeue mode. The no operation of this command will reset it to default value. At the same time, reset the weight of the output queue to default value.

Parameters:

None

Default:

Non priority-queue mode.

Command Mode:

Interface Configuration Mode.

Usage Guide:

When adopting priority-queue as dequeue mode, the WRR weighting algorithm will not be used to send messages. Instead, messages from the low-priority queue can only be sent after those ones from the high-priority queue are all sent.

Examples:

Set the dequeue mode of port ethernet1/1as priority-queue mode.

```
Switch(Config-If-Ethernet1/1)#priority-queue out
```

14.9 queue bandwidth

Command:

queue-bandwidth <queue-id> <min_kbits_per_second> <max_kbits_per_second>

no queue-bandwidth <queue-id>

Function:

Configure the bandwidth pledge for the egress queue.

Parameter:

<queue-id> is the queen ID to configure the bandwidth pledge, the different chip supports the different queue count, the range is difference too, the normal state is 8 queue, and the ranging from 1 to 8. **<min_kbits_per_second>** is the min-bandwidth, ranging from 0 to 128000, when input 0, it means the min-bandwidth function is not take effect. **<max_kbits_per_second>** is the max-bandwidth, ranging from 0 to 128000, when input 0, it means the max-bandwidth function is not take effect. But the min-bandwidth and max-bandwidth are not allowed to input 0 at the same time, and the min-bandwidth must not bigger than max-bandwidth.

Default:

The queue bandwidth have no pledge by default.

Command mode:

Interface Mode

Usage Guide:

The min-bandwidth pledge and max-bandwidth limit can be configured at the different or same queue. For example: the queue1 bandwidth of ethernet1/2 is limited as 128kbps, it just need to configure queue-bandwidth 1 0 128.

The queue bandwidth pledge for egress is relative to remove mode, for example: one port is the strict priority-queue, the highest priority is queue 1 now, it will satisfy this queue traffic when block is happened. But if user want the lower priority of queue having bandwidth, it can remain bandwidth via this command, the lower priority queue's min-bandwidth will be satisfied at first, then the excess bandwidth is removed according to PQ.

Example:

Configure the min-bandwidth is 64kbps and the max-bandwidth is 128kbps for ethernet1/2 queue1.

```
Switch(config)#interface ethernet 1/2
```

```
Switch(Config-If-Ethernet1/2)#queue-bandwidth 1 64 128
```

14.10 set

Command:

set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>| ipv6 dscp <new-dscp> | ipv6 flowlabel <new-flowlabel> | ip nexthop <ip-address> | cos <*new-cos*>}

no set {ip *dscp <new-dscp*> | ip precedence <new-precedence> | ipv6 dscp <new-dscp> | ipv6 flowlabel <new-flowlabel> | ip nexthop <ip-address> | cos }

Function:

Assign a new DSCP, IP Precedence for the classified traffic; the “no” form of this command delete assigning the new values.

Parameter:

ip dscp <*new-dscp*> new DSCP value; **ip precedence <*new-precedence*>** new IPv4 Precedence; **ipv6 dscp <*new-dscp*>** new IPv6 DSCP value; **ipv6 flowlabel <new-flowlabel>** new IPv6 FL value. **ip nexthop <*ip-address*>** next hop IP address, set the route of nexthop for PBR. **cos <*new cos*>** new COS value.

Default:

Not assigning by default.

Command Mode:

Policy Class-map Mode

Usage Guide:

Only the classified traffic which matches the matching standard will be assigned with the new values.

Note: ipv6 flowlabel configuration is not supported by this switch.

Example:

Set the IP DSCP of the packets matching the c1 class rule to 3.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

14.11 service-policy

Command:

service-policy input <*policy-map-name*>

no service-policy input <*policy-map-name*>

Function:

Applies a policy map to the specified port or VLAN interface; the no command deletes the specified policy map applied to the port or VLAN interface.

Parameters:

input <policy-map-name> applies the specified policy map to the ingress redirection of switch port or VLAN interface.

Default:

No policy map is bound to port and VLAN interface by default.

Command mode:

Interface Configuration Mode(Switch port or VLAN interface).

Usage Guide:

Configuring port trust status and applying policy map on the port are two conflicting operations; the later configuration will override the earlier configuration. Only one policy map can be applied to each direction of each port or VLAN interface. Egress policy map is not supported yet.

Example:

Bind policy p1 to ingress Ethernet port 1/1.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

Bind policy p1 to ingress redirection of v1 interface.

```
Switch(config)#interface vlan 1
Switch(Config-If-vlan1)#service-policy input p1
```

14.12 show class-map

Command:

show class-map [<*class-map-name*>]

Function:

Displays class map of QoS.

Parameters:

< *class-map-name*> is the class map name.

Default:

N/A.

Command mode:

Admin Mode.

Usage Guide:

Displays all configured class-map or specified class-map information.

Example:

```
Switch # show class-map
Class map name:c1, used by 1 times
   match acl name:1
```

Displayed information Explanation
Class map name:c1 Name of the Class map
used by 1 times Used times
match acl name:1 Classifying rule for the class map.

14.13 show policy-map

Command:

show policy-map [<*policy-map-name*>]

Function:

Displays policy map of QoS.

Parameters:

<policy-map-name> is the policy map name.

Default:

N/A.

Command mode:

Admin Mode.

Usage Guide:

Displays all configured policy-map or specified policy-map information.

Example:

Displays policer information of non-aggregate.

```
Switch#show policy -map
Policy Map p1
  Class Map name: c1
  police 16000000 2000 conform-action drop exceed-action transmit
```

Displayed information Explanation
Policy Map p1 Name of policy map
Class map name:c1

Name of the class map referred to
police 16000000 2000 conform-action drop exceed-action transmit Policy implemented

14.14 show mls qos aggregate-policy

Command:

show mls qos aggregate-policy [<*aggregate-policy-name*>]

Function:

Displays policy set configuration information for QoS.

Parameters:

<aggregate-policy-name> is the policy set name.

Default:

N/A.

Command mode:

Admin and Configuration Mode.

Usage Guide:

Displays all QoS policy or specified QoS policy information.

Example:

```
Switch(config)#show mls qos aggregate-policy a2
aggregate policy a2 10 10 10 conform-action set-dscp-transmit 7
Not used by any policy map
```

Displayed information Explanation
aggregate policy a2 10 10 10 conform-action set-dscp-transmit 7 Configuration for this policy set.
Not used by any policy map Time that the policy set is being referred to

14.15 show mls qos interface

Command:

show mls qos interface [<*interface-id*>] [buffers | policy | queuing | statistics]

Function:

Displays QoS configuration information on a port.

Parameters:

<interface-id> is the port ID; **buffers** is the queue buffer setting on the port; **policy** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.

Default:

N/A.

Command mode:

Admin Mode.

Usage Guide:

In single rate single bucket mode, the messages can only red or green when passing police. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of messages. But the counter can only count two kinds of messages, the red and yellow ones will both be treated as out-profile. Only when configuring ingress policies, there is statistic information.

Example:

```
Switch #show mls qos interface ethernet 1/2
Ethernet 1/2
    default cos:0
    DSCP Mutation Map: Default DSCP Mutation Map
Attached policy map for Ingress: p1
```

Displayed information Explanation
Ethernet1/2 Port name
default cos:0 Default CoS value of the port.
DSCP Mutation Map: Default DSCP Mutation Map Port DSCP map name
Attached policy map for Ingress: p1 Policy name bound to port.

```
Switch # show mls qos interface buffers ethernet 1/2
Ethernet 1/2
            packet    number of 8 queue:
            0x200 0x200 0x200 0x200 0x200 0x200 0x200
```

0x200 Displayed information Explanation
Ethernet1/2 Port name
packet number of 8 queue: 0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200 Available packet number for all 8 queues out on the port, this is a fixed setting that cannot be changed.

Switch # show mls qos interface queuing ethernet 1/2

Cos-queue map:

Cos	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Queue and weight type:

Port	q1	q2	q3	q4	q5	q6	q7	q8	QType
Ethernet1/2	1	2	3	4	5	6	7	8	WRR

Displayed information Explanation
Cos-queue map: CoS value to queue mapping.
Queue and weight type: Queue to weight mapping.
QType WRR or PQ queue out method

Switch # show mls qos interface policy ethernet 1/2

Ethernet1/2

```
Attached policy map for Ingress: p1
```

Displayed information Explanation
Ethernet1/2 Port name
Attached policy map for Ingress: p1 Policy map bound to the port.

```
Switch # show mls qos interface statistics ethernet 1/2
Device: Ethernet 1/2
    Classmap      classified      in-profile      out-profile (in packets)
        c1              0               0               0
```

Displayed information Explanation
Ethernet1/2 Port name
ClassMap Name of the Class map
Classified Total data packets match this class map.
In-profile Total in-profile data packets match this class map.
out-profile Total out-profile data packets match this class map.

14.16 show mls qos maps

Command:

show mls qos maps policed-dscp [normal-burst|max-burst]

Function:

Display the configuration of policed-dscp map.

Parameters:

normal-burst map for the yellow messages. max-burst map for the red messages. No parameter means to print both maps

Default:

N/A.

Command mode:

Admin and Config Mode.

Usage Guide:

Display the map configuration information of QoS.

Example:

Display configuration information of policed-dscp mapping table.

```
Switch(config)#show mls qos maps policed-dscp
Normal Burst Policed-dscp map:
        d1 : d2 0   1   2   3   4   5   6   7   8   9
        0:       0   1   2   3   4   5   6   7   8   9
        1:      10 11 12 13 14 15 16 17 18 19
        2:      20 21 22 23 24 25 26 27 28 29
        3:      30 31 32 33 34 35 36 37 38 39
        4:      40 41 42 43 44 45 46 47 48 49
        5:      50 51 52 53 54 55 56 57 58 59
        6:      60 61 62 63

Maximum Burst Policed-dscp map:
        d1 : d2 0   1   2   3   4   5   6   7   8   9
        0:       0   7   7   7   7   7   6   7   8   9
        1:      10 11 12 13 14 15 16 17 18 19
        2:      20 21 22 23 24 25 26 27 28 29
        3:      30 31 32 33 34 35 36 37 38 39
        4:      40 41 42 43 44 45 46 47 48 49
        5:      50 51 52 53 54 55 56 57 58 59
        6:      60 61 62 63
```

14.17 show mls-qos

Command:

show mls-qos

Function:

Displays global configuration information for QoS.

Parameters:

N/A.

Default:

N/A.

Command mode:

Admin Mode.

Usage Guide:

This command indicates whether QoS is enabled or not.

Example:

```
Switch#show mls-qos
Qos is enabled!
```

Displayed information	Explanation
Qos is enabled!	Qos function is enabled!

14.18 wrr-queue bandwidth

Command:

wrr-queue bandwidth *<weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8>*

no wrr-queue bandwidth

Function:

Sets the WRR weight for specified egress queue; the '**no queue bandwidth'** command restores the default setting.

Parameters:

<weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8> are WRR weights, ranging from 0 to 15.

Default:

The default values of weight1 to weight8 are 1 through 8.

Command mode:

Interface Configuration Mode.

Usage Guide:

The absolute value of WRR is meaningless. WRR allocates bandwidth by using eight weight values. If a weight is 0, then the queue has the highest priority; when the weights of multiple queues are set to 0, then the queue of higher order has the higher priority.

Notice:

Only one or two queues can be set 0, and the queues which be set to 0 are at back.

Example:

Setting the bandwidth weight proportion of the eight queue out to be 1:1:2:2:4:4:8:8.

```
Switch(Config-If-Ethernet1/1)#wrr-queue bandwidth1 1 2 2 4 4 8 8
```

14.19 wrr-queue cos-map

Command:

wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>

no wrr-queue cos-map

Function:

Sets the CoS value mapping to the specified queue out; the "**no wrr-queue cos-map**" command restores the default setting.

Parameters:

<queue-id> is the ID of queue out, ranging from 1 to 8; ***<cos1 ... cos8>*** are CoS values mapping to the queue out, ranging from 0-7, up to 8 values are supported.

Default:

efault CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	0	1	2	3	4	5	6	7
Queue Selected	1	2	3	4	5	6	7	8

Command mode:

Global Mode

Usage Guide:

When global QoS is close by default mapping value.

Example:

Mapping packets with CoS value 2 and 3 to egress queue 1.

```
Switch(config)#wrr-queue cos-map 1 2 3
```

Chapter 15 Commands for IPv6 PBR

15.1 class

Command:

class <*class-map-name*>

no class <*class-map-name*>

Function:

Correlate a class, and enter policy-class-map mode; the **no class <*class-map-name*>**will delete the specified policy-class-map.

Parameters:

<class-map-name> specify the class-map name adopted by the policy-class-map.

Default:

There is no policy-class-map by default.

Command Mode:

Policy-class-map Mode.

Usage Guide:

Before creating a policy-class-map, users should create a policy-map and enter policy-map mode first; in policy-class-map mode, users can class the packet flows classed according to the class-map and configure the next hop for them.

Example:

Enter a policy-class-map mode.

Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#exit

15.2 class-map

Command:

class-map <*class-map-name*>

no class-map <*class-map-name*>

Function:

Create a class-map, enter class-map mode; the **no class-map <*class-map-name*>** will delete the specified class-map.

Parameters:

<class-map-name> the name of the class-map.

Default:

There is no class-map by default.

Command Mode:

Global Configuration Mode

Usage Guide:

None.

Example:

Create and delete a class-map named as c1.

```
Switch(config)#class-map    c1
Switch(config-ClassMap)# exit
Switch(config)#no class-map c1
```

15.3 mls qos

Command:

mls qos

no mls qos

Function:

Globally enable QoS, and then PBR will be enabled too. The **no mls qos** will globally disable QoS, PBR will be disabled too.

Command Mode:

Global Configuration Mode.

Default:

Disable PBR.

Usage Guide:

While enabling and disabling QoS function, PBR function will automatically enabled and disabled. PBR can not be enabled or disabled alone.

Example:

Enable and disable QoS and PBR function.

```
Switch(config)#mls qos
```

15.4 match ipv6 access-group

Command:

match ipv6 access-group <*acl-index-or-name*>

no match ipv6 access-group

Function:

Set the match standard in the class-map; the **no match ipv6 access-group** will delete the specified match standard.

Parameters:

access-group <*acl-index-or-name*> match the specified ACL list, the parameter is the index or name of the ACL.

Default:

There is no match standard by default.

Command Mode:

Class-map Mode.

Usage Guide:

There can only be one match standard in each class-map. For the ACL list applied in PBR, the permit action and denies action in the entries means specify or don't specify the next hop for the IPv6 message meeting the match standard.

Example:

Create a class-map named as c1, set the classing rule of this class-map as matching the messages whose access-group is a1.

```
Switch(config)#class-map c1
Switch(config-ClassMap)# match ipv6 access-group a1
Switch(config-ClassMap)#exit
```

15.5 policy-map

Command:

policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Function:

Create a policy-map and enter policy-map mode; the **no policy-map <*policy-map-name*>** will delete the specified policy-map.

Parameters:

<policy-map-name> the name of the policy-map.

Default:

There is no policy-map by default.

Command Mode:

Global Configuration Mode.

Usage Guide:

After entering policy-map mode, users can do a series of operations like the class match of PBR or setting the next hop and so on.

Examples:

Create and delete a policy-map named as p1.

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#exit
Switch(config)#no policy-map p1
```

15.6 set

Command:

set {ipv6 nexthop <*nexthop-ip*>}

no set {ipv6 nexthop}

Function:

Set the next hop IP for the classed flows; the **no set {ipv6 nexthop}** will cancel the new set value.

Parameters:

<nexthop-ip> the next hop IP, which has to be a global trunk unicast address.

Default:

There is no configuration by default.

Command Mode:

Policy-class-map Mode.

Usage Guide:

The policy of setting the next hop IP can only adopt the class-map matching IPv6 ACL.

Example:

Set the next hop of the messages meeting c1 classing rules as 3ffe:506::.

Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#set ip nexthop 3ffe:506::
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit

15.7 service-policy

Command:

service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function:

Apply a policy-map on a switch port; the no operation of this command will delete a specified policy-map applied to the switch port.

Parameters:

input <*policy-map-name*> applies the policy-map with the specified name to the input of the switch port; **output <*policy-map-name*>** applies the policy-map with the specified name to the output of the switch port.

Default:

There is no bound policy-map by default.

Command Mode:

Port Configuration Mode.

Usage Guide:

Configuring the trust state of a port is mutually exclusive to applying policy-map on a port, the later configuration will overwrite the former one; there can be only one policy-map on each direction of a port. The output policy-map is not supported at present.

Example:

Bind policy p1 to the input of ethernet1/1.

```
Switch(config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# service-policy input p1
```

Chapter 16 Commands for Flow-based Redirection

16.1 access-group redirect to interface ethernet

Command:

access-group <*aclname*> redirect to interface [ethernet <*IFNAME*> | <*IFNAME*>]

no access-group <*aclname*> redirect

Function:

Specify flow-based redirection; “no access-group <aclname> redirect” command is used to delete flow-based redirection.

Parameters:

<aclname> name of the flow , only supports digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Parameters of **Timerange** and **Portrange** can not be set in ACL, the type of ACL should be Permit. ***<IFNAME>*** the destination port of redirection.

Command Mode:

Physical Interface Configuration Mode.

Usage Guide:

“no access-group <aclname> redirect” command is used to delete flow-based redirection. Flow-based redirection function enables the switch to transmit the data frames meeting some special condition to another specified port.

Examples:

Redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6,

Switch(config)#access-list 1 permit host 192.168.1.111
Switch(config)# interface ethernet 1/1
Switch(Config-If-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6

16.2 show flow-based-redirect

Command:

show flow-based-redirect {interface [ethernet <*IFNAME*> | <*IFNAME*>]}

Function:

Display the information of current flow-based redirection in the system/port.

Parameters:

1. No specified port, display the information of all the flow-based redirection in the system.
2. Specify ports in ***<IFNAME>***, display the information of the flow-based redirection configured in the ports listed in the interface-list.

Command Mode:

Admin Mode and Configuration Mode.

Usage Guide:

This command is used to display the information of current flow-based redirection in the system/port.

Examples:

```
Switch(config)# show flow-based-redirect
```

Flow-based-redirect config on interface ethernet 1/1:

RX flow (access-list 1) is redirected to interface Ethernet1/6

Chapter 17 Commands for Layer 3 Forwarding

17.1 Commands for Layer 3 Interface

17.1.1 bandwidth

Command:

bandwidth *<bandwidth>*

no bandwidth

Function:

Configure the bandwidth for Interface vlan. The "**no bandwidth**" command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth（cost=10^8/bandwidth）when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.

Parameters:

<bandwidth> is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit "k, m, g". There are no decimal numbers after conversion.

Command mode:

VLAN Interface Mode

Default:

The default bandwidth for interface VLAN is 100,000,000bit.

Usage Guide:

This command only can be used at interface VLAN mode。The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.

Example:

Configure the bandwidth for vlan1 is 50,000,000bit.

```
Switch(Config-if-Vlan1)#bandwidth 50m
```

17.1.2 shutdown

Command:

shutdown

no shutdown

Function:

Shut down the specified VLAN interface of the switch. The no operation of the command will enable the VLAN interface.

Command Mode:

VLAN Interface Configuration Mode.

Default:

The VLAN interface is enabled by default.

Usage Guide:

While shutting down the VLAN interface of the switch, it will not send data frames. If this interface needs to obtain an IP address via BOOTP/DHCP protocol, it should be enabled.

Example:

Enable the VLAN1 interface of the switch.

```
Switch(Config-if-Vlan1)#no shutdown
```

17.1.3 interface vlan

Command:

interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function:

Create a VLAN interface (a Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the Layer 3 interface specified.

Parameters:

<vlan-id> is the VLAN ID of the established VLAN, ranging from 1 to 4094.

Default:

No Layer 3 interface is configured upon switch shipment.

Command mode:

Global Mode

Usage Guide:

When creating a VLAN interface (Layer 3 interface), VLANs should be configured first, for details, see the VLAN chapters. When VLAN interface (Layer 3 interface) is created with this command, the VLAN interface (Layer 3 interface) configuration mode will be entered. After the creation of the VLAN interface (Layer 3 interface), interface vlan command can still be used to enter Layer 3 Port Mode.

Example:

Creating a VLAN interface (layer 3 interface).

```
Switch (config)#interface vlan 1
```

17.1.4 interface loopback

Command:

interface loopback <*loopback-id*>

no interface loopback <*loopback-id*>

Function:

Create a Loopback interface; the no operation of this command will delete the specified Loopback interface.

Parameters:

<loopback-id> is the ID of the new created Loopback interface.

Default:

There is no Loopback interface in factory defaults.

Command Mode:

Global Configuration Mode.

Usage Guide:

IDs of the VLANs taken up by a Loopback interfaces start from 1006. If Loopback take up a VLAN whose ID is larger than or equal with1006, users are forbidden to configure the corresponding VLAN. If a VLAN after VLAN 1006 is already configured, such as VLAN 1006, then the Loopback interface will take up the first available VLAN after that VLAN, such as VLAN 1007.

Examples:

Enter the interface configuration mode of Loopback 1.

```
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#
```

17.2 Commands for IPv4/v6 configuration

17.2.1 clear ipv6 neighbor

Command:

clear ipv6 neighbors

Function:

Clear the neighbor cache of IPv6.

Parameter:

None

Command Mode:

Admin Mode

Default:

None

Usage Guide:

This command can not clear static neighbor.

Example:

Clear neighbor list.

```
Switch#clear ipv6 neighbors
```

17.2.2 debug ip packet

Command:

debug ip packet

no debug ip packet

Function:

Enable the IP packet debug function: the "**no debug IP packet**" command disables this debug function.

Parameter:

None

Default:

IP packet debugging information is disabled by default.

Command mode:

Admin Mode

Usage Guide:

Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.

Example:

Enabling IP packet debug.

```
Switch#debug ip pa
```

IP PACKET: rcvd, src1.1.1.1, dst1.1.1.2, size 100

17.2.3 debug ipv6 packet

Command:

debug ipv6 packet

no debug ipv6 packet

Function:

IPv6 data packets receive/send debug message.

Parameter:

None

Default:

None

Command Mode:

Admin Mode

Usage Guide:

None

Example:

```
Switch#debug ipv6 packet
IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>,
from Vlan1
```

Displayed information Explanation
IPv6 PACKET: rcvd Receive IPv6 data report
Src <fe80::203:fff:fe01:2786> Source IPv6 address
Dst <fe80::1> Destination IPv6 address

size <64> Size of data report
proto <58> Protocol field in IPv6 header
from Vlan1 IPv6 data report is collected from Layer 3 port vlan1

17.2.4 debug ipv6 icmp

Command:

debug ipv6 icmp

no debug ipv6 icmp

Function:

ICMP data packets receive/send debug message.

Parameter:

None

Default:

None

Command Mode:

Admin Mode

Example:

```
Switch#debug ipv6 icmp
IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1
```

Displayed information Explanation
IPv6 ICMP: sent Send IPv6 data report
type <129> Ping protocol No.
Src <2003::1> Source IPv6 address
Dst <2003::20a:ebff:fe26:8a49> Destination IPv6 address

from Vlan1 Layer 3 port being sent

17.2.5 debug ipv6 nd

Command:

debug ipv6 nd [ns | na | rs | ra | redirect]

no debug ipv6 nd [ns | na | rs | ra | redirect]

Function:

Function: Enable the debug of receiving and sending operations for specified types of IPv6 ND messages. The ns, na, rs, ra and redirect parameters represent neighbor solicitation, neighbor advertisement, route solicitation, route advertisement and route redirect. No specification means to enable the debug for all five types of ND message. The no operation of this command will disable debug of receiving and sending operations for specified types of IPv6 ND messages, while no specification means to disable that for all five types of ND message.

Parameter:

None.

Default:

The debug of receiving and sending operations for all five types of IPv6 ND messages is disabled by default.

Command Mode:

Admin Mode

Usage Guide:

The ND protocol is an essential part of IPv6. This command can display the ND message of a specified type for troubleshooting.

Example:

```
Switch#debug ipv6 nd
    IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst
<fe80::203:fff:fe01:59ba>
```

Displayed information Explanation
IPv6 ND: rcvd Receive ND data report
type <136> ND Type
Src <fe80::203:fff:fe01:2786> Source IPv6 address

Dst <fe80::203:fff:fe01:59ba> Destination IPv6 address

17.2.6 debug ipv6 tunnel packet

Command:

debug ipv6 tunnel packet

no debug ipv6 tunnel packet

Function:

tunnel data packets receive/send debug message.

Parameter:

None

Default:

None

Command Mode:

Admin Mode

Example:

```
Switch#debug ipv6 tunnel packet
```

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

Displayed information Explanation
IPv6 tunnel packet : rcvd Receive tunnel data report
type <136> ND type
Src 178.1.1.1 dst Tunnel source IPv4 address
Dst 179.2.2.2 Tunnel destination IPv4 address

17.2.7 ipv6 enable

Command:

ipv6 enable

no ipv6 enable

Function:

This command enables functions such as Unicast IPv6 Data Packet Transmit, Neighbor Discovery, Router advertisement and Routing Protocol, etc.

Parameter:

None

Command Mode:

Global Mode

Default:

IPv6 is disabled.

Usage Guide:

To enable ipv6 enable command will allow configuring IPv6 command and process IPv6 data transmission.

Example:

Turn on IPv6 Enable switch under Global Mode.

```
Switch(config)#ipv6 enable
```

17.2.8 ipv6 proxy enable

Command:

ipv6 proxy enable

no ipv6 proxy enable

Function:

This command enable the IPv6 proxy function of a chassis switch. The no operation of this command will disable IPv6 proxy function.

Parameter:

None.

Command Mode:

Global Configuration Mode.

Default:

The IPv6 proxy function in the system is disabled by default.

Usage Guide:

IPv6 proxy function means that, the board cards supporting IPV4 only will forward the IPv6 packets to the IPV6-supporting board cards in the system, implementing a process of wire-speed forwarding. The proxy provided by IPv6 board cards indirectly realizes the Ipv6 hardware routing and forwarding function implemented by earlier board cards which only support IPv4.

Notice:

if the IPv6 proxy function is enabled, at least one board cards supporting IPv6 hardware forwarding should be plugged into the chassis switch. If all board cards in the chassis switch support IPv6 hardware forwarding, there would be no need to use the IPv6 proxy function. At present, the IPv6 proxy function does not support the proxy forwarding of IPv6 tunnel messages and multicast data messages

Examples:

Enable the IPv6 proxy function.

```
Switch(config)#ipv6 proxy enable
```

17.2.9 ip address

Command:

ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function:

Set IP address and net mask of switch; the "**no ip address [<*ip-address*> <*mask*>] [secondary]**" command deletes the IP address configuration.

Parameter:

<ip-address> is IP address, dotted decimal notation;

<mask> is subnet mask, dotted decimal notation;

[secondary] indicates that the IP address is configured as secondary IP address.

Command Mode:

VLAN interface configuration mode

Default:

The system default is no IP address configuration.

Usage Guide:

This command configures IP address on VLAN interface manually. If optional parameter **secondary** is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.

Example:

The IP address of switch VLAN1 interface is set to 192.168.1.10/24.

```
Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0
```

17.2.10 ipv6 address

Command:

ipv6 address <*ipv6-address*|*prefix-length*> [eui-64]

no ipv6 address <*ipv6-address*|*prefix-length*> [eui-64]

Function:

Configure aggregately global unicast address, site-local address and link-local address for the interface.

Parameter:

Parameter ***<ipv6-address>*** is the prefix of IPv6 address, parameter ***<prefix-length>*** is the prefix length of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface.

Command Mode:

Interface Configuration Mode.

Default:

None.

Usage Guide:

IPv6 address prefix can not be multicast address or any other specific IPv6 address, and different layer 3 interfaces can not configure the same address prefix. For global unicast address, the prefix must be in the range from 2000:: to 3fff::, and the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 3. For interface loopback port, the length of the prefix must be equaled to 128.

Example:

Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64.

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

17.2.11 ipv6 route

Command:

ipv6 route <*ipv6-prefix* | *prefix-length*> {<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]

no ipv6 route <*ipv6-prefix* | *prefix-length*> {<*ipv6address*> | <*interface-type interface-number*> | {<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]

Function:

Set IPv6 static route.

Parameters:

Parameter ***<ipv6-prefix>*** is the destination prefix of IPv6 static route, parameter ***<prefix-length>*** is the length of IPv6 prefix, parameter ***<ipv6-address>*** is the next hop IPv6 address of the reachable network, parameter ***<interface-type interface-number>*** is the name of interface from which to reach the destination, ***<tunnel no>*** is the output tunnel number of the tunnel route, parameter ***<precedence>*** is the weight of this route, the range is 1-255, the default is 1

Default:

There is not any IPv6 static route which is configured by default.

Command Mode:

Global Mode

Usage Guide:

When the next hop IPv6 address is link-local address, the interface name must be specified. When the next hop IPv6 address is global aggregatable unicast address and site-local address, if no interface name of the exit is specified, it must be assured that the IP address of the next hop and the address of some interface of the switch must be in the same network segment. As for tunnel route, interface name can be directly specified.

Example:

Configure static route 1 with destination address 3ffe:589:dfc::88, prefix length 64 and next hop 2001:8fd:c32::99 (the router has been configured IPv6 address of 2001:8fd:c32::34/64).

```
Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99
```

Configure static route 2 with destination 3ffe:ff7:123::55, prefix length 64, next hop fe80::203:ff:89fd:46ac and exit interface name Vlan1.

```
Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1
```

17.2.12 ipv6 redirect

Command:

ipv6 redirect

no ipv6 redirect

Function:

Enable IPv6 router redirect function. The no operation of this command will disable the function.

Parameters:

None.

Command Mode:

Global Configuration Mode.

Default Settings:

IPv6 router redirect function is disabled by default.

Usage Guide:

If router A, router B, and node C are on the same network link, and router A forwards IPv6 packets from node C to router B, expecting router B to continue the forwarding, then router A will send an IPv6 ICMPv6 redirect message to node C-source of the packet, notifying it that the best next hop of this destination address is router B. By doing so, the forwarding overhead of router A will be decreased, so is the network transmission delay of node C.

Examples:

Enable IPv6 router redirect function.

```
Switch(config)# ipv6 redirect
```

17.2.13 ipv6 nd dad attempts

Command:

ipv6 nd dad attempts <*value*>

no ipv6 nd dad attempts

Function:

Set Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection.

Parameter:

<value> is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection, and the value of ***<value>*** must be in 0-10, NO command restores to default value 1.

Command Mode:

Interface Configuration Mode

Default:

The default request message number is 1.

Usage Guide:

When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, *value* being 0 means no Duplicate Address Detection is executed.

Example:

The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3.

```
Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3
```

17.2.14 ipv6 nd ns-interval

Command:

ipv6 nd ns-interval <*seconds*>

no ipv6 nd ns-interval

Function:

Set the time interval of Neighbor Solicitation Message sent by the interface.

Parameter:

parameter ***<seconds>*** is the time interval of sending Neighbor Solicitation Message, ***<seconds>*** value must be between 1-3600 seconds, **no** command restores the default value 1 second.

Command Mode:

Interface Configuration Mode

Default:

The default Request Message time interval is 1 second.

Default:

The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.

Example:

Set Vlan1 interface to send out Neighbor Solicitation Message time interval to be 8 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8
```

17.2.15 ipv6 nd suppress-ra

Command:

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Function:

Prohibit router announcement.

Parameter:

None

Command Mode:

Interface Configuration Mode

Default:

Router Announcement function is disabled.

Usage Guide:

no ipv6 nd suppress-ra command enable router announcement function.

Example:

Enable router announcement function.

```
Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra
```

17.2.16 ipv6 nd ra-lifetime

Command:

ipv6 nd ra-lifetime <*seconds*>

no ipv6 nd ra-lifetime

Function:

Configure the lifetime of router announcement.

Parameter:

parameter ***<seconds>*** stands for the number of seconds of router announcement lifetime, ***<seconds>*** value must be between 0-9000.

Command Mode:

Interface Configuration Mode

Default:

The number of seconds of router default announcement lifetime is 1800.

Usage Guide:

This command is used to configure the lifetime of the router on Layer 3 interface, seconds being 0 means this interface can not be used for default router, otherwise the value should not be smaller than the maximum time interval of sending router announcement. If no configuration is made, this value is equal to 3 times of the maximum time interval of sending routing announcement.

Example:

Set the lifetime of routing announcement is 100 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd ra-lifetime 100
```

17.2.17 ipv6 nd min-ra-interval

Command:

ipv6 nd min-ra-interval <*seconds*>

no ipv6 nd min-ra-interval

Function:

Set the minimum time interval of sending routing message.

Parameter:

Parameter ***<seconds>*** is number of seconds of the minimum time interval of sending routing announcement, ***<seconds>*** must be between 3-1350 seconds.

Command Mode:

Interface Configuration Mode

Default:

The default minimum time interval of sending routing announcement is 200 seconds.

Usage Guide:

The minimum time interval of routing announcement should not exceed 3/4 of the maximum time interval.

Example:

Set the minimum time interval of sending routing announcement is 10 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd min-ra-interval 10
```

17.2.18 ipv6 nd max-ra-interval

Command:

ipv6 nd max-ra-interval <*seconds*>

no ipv6 nd max-ra-interval

Function:

Set the maximum time interval of sending routing message.

Parameter:

Parameter ***<seconds>*** is number of seconds of the time interval of sending routing announcement, ***<seconds>*** must be between 4-1800 seconds.

Command Mode:

Interface Configuration Mode

Default:

The default maximum time interval of sending routing announcement is 600 seconds.

Usage Guide:

The maximum time interval of routing announcement should be smaller than the lifetime value routing announcement.

Example:

Set the maximum time interval of sending routing announcement is 20 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd max-ra-interval 20
```

17.2.19 ipv6 nd prefix

Command:

ipv6 nd prefix *<ipv6-prefix | prefix-length>*{ [*<valid-lifetime> <preferred-lifetime>*] [no-autoconfig | off-link[no-autoconfig]]}

no ipv6 nd prefix *<ipv6-prefix | prefix-length>*

Function:

Configure the address prefix and relative parameters for router announcement.

Parameter:

Parameter ***<ipv6-prefix>*** is the address prefix of the specified announcement, parameter ***<prefix-length>*** is the length of the address prefix of the specified announcement, parameter ***<valid-lifetime>*** is the valid lifetime of the prefix, parameter ***<preferred-lifetime>*** is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime. Parameter **no-autoconfig** says this prefix can not be used to automatically configure IPv6 address on the host in link-local. Parameter **off-link** says the prefix specified by router announcement message is not assigned to link-local, the node which sends data to the address including this prefix consider link-local as unreachable.

Command Mode:

Interface Configuration Mode

Default:

The default value of ***valid-lifetime*** is 2592000 seconds (30 days), the default value of ***preferred-lifetime*** is 604800 seconds (7 days). **off-link** is off by default, **no-autoconfig** is off by default.

Usage Guide:

This command allows controlling the router announcement parameters of every IPv6 prefix. Note that valid lifetime and preferred lifetime must be configured simultaneously.

Example:

Configure IPv6 announcement prefix as 2001:410:0:1::/64 on Vlan1, the valid lifetime of this prefix is 8640 seconds, and its preferred lifetime is 4320 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320
```

17.2.20 ipv6 nd ra-hoplimit

Command:

ipv6 nd ra-hoplimit <value>

Function:

Set the hoplimit of sending router advertisement.

Parameters:

<value> is the hoplimit of sending router advertisement, ranging from 1 to 255.

Command Mode：

Interface Configuration Mode.

Default:

The default hoplimit of sending router advertisement is 64.

Example:

Set the hoplimit of sending router advertisement in interface vlan 1 as 128.

```
Switch#(Config-if-Vlan1)#ipv6 nd ra-hoplimit 128
```

17.2.21 ipv6 nd ra-mtu

Command:

ipv6 nd ra-mtu <value>

Function:

Set the mtu of sending router advertisement.

Parameters:

<value> is the mtu of sending router advertisement, ranging from 0 to 1500.

Command Mode：

Interface Configuration Mode.

Default:

The default mtu of sending router advertisement is 1500.

Example:

Set the mtu of sending router advertisement in interface vlan 1 as 500.

```
Switch#(Config-if-Vlan1)#ipv6 nd ra-mtu 500
```

17.2.22 ipv6 nd reachable-time

Command:

ipv6 nd reachable-time <seconds>

Function:

Set the reachable-time of sending router advertisement.

Parameters:

<value> is the reachable-time of sending router advertisement, ranging from 0 to 3600000 milliseconds.

Command Mode：

Interface Configuration Mode.

Default Settings:

The default reachable-time of sending router advertisement is 30000 milliseconds.

Example:

Set the reachable-time of sending router advertisement in interface vlan 1 as 100000 milliseconds.

```
Switch#(Config-if-Vlan1)#ipv6 nd reachable-time 100000
```

17.2.23 ipv6 nd retrans-timer

Command:

ipv6 nd retrans-timer <seconds>

Function:

Set the retrans-timer of sending router advertisement.

Parameters:

<value> is the retrans-timer of sending router advertisement, ranging from 0 to 4294967295 milliseconds.

Command Mode:

Interface Configuration Mode.

Default:

The default retrans-timer of sending router advertisement is 1000 milliseconds.

Example:

Set the reachable-time of sending router advertisement in interface vlan 1 as 10000 milliseconds.

```
Switch#(Config-if-Vlan1)#ipv6 nd retrans-timer 10000
```

17.2.24 ipv6 nd other-config-flag

Command:

ipv6 nd other-config-flag

Function:

Set the flag representing whether information other than the address information will be obtained via DHCPv6.

Parameters:

None.

Command Mode：

Interface Configuration Mode.

Default:

Information other than the address information won't be obtained via DHCPv6.

Examples:

Set IPv6 information other than the address information in interface vlan 1 will be obtained via DHCPv6.

```
Switch#(Config-if-Vlan1)#ipv6 nd other-config-flag
```

17.2.25 ipv6 nd managed-config-flag

Command:

ipv6 nd managed-config-flag

Function:

Set the flag representing whether the address information will be obtained via DHCPv6.

Parameters:

None.

Command Mode：

Interface Configuration Mode.

Default:

The address information won't be obtained via DHCPv6.

Examples:

Set IPv6 address information in interface vlan 1 will be obtained via DHCPv6.

```
Switch#(Config-if-Vlan1)#ipv6 nd managed-config-flag
```

17.2.26 ipv6 neighbor

Command:

ipv6 neighbor *<ipv6-address>* *<hardware-address>* interface *<interface-type interface-number>*

no ipv6 neighbor *<ipv6-address>*

Function:

Set static neighbor table entry.

Parameters:

Parameter ***ipv6-address*** is static neighbor IPv6 address, same to interface prefix parameter, parameter ***hardware-address*** is static neighbor hardware address, ***interface-type*** is Ethernet type, ***interface-number*** is Layer 2 interface name.

Command Mode:

Interface Configuration Mode

Default Situation:

There is not static neighbor table entry.

Usage Guide:

IPv6 address and multicast address for specific purpose and local address can not be set as neighbor.

Example:

Set static neighbor 2001:1:2::4 on port E1/1, and the hardware MAC address is 00-30-4f-89-44-bc.

```
Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-30-4f-89-44-bc interface Ethernet 1/1
```

17.2.27 ipv6 rthdr-type0 enable

Command:

ipv6 rthdr-type0 enable

no ipv6 rthdr-type0 enable

Function:

Enable the Ipv6 type 0 route header (RH0) handling function. The no operation of this command will disable the IPv6 type 0 route header (RH0) handling function.

Parameters:

None.

Command Mode:

Global Configuration Mode.

Default:

The IPv6 type 0 route header handling function is disabled by default.

Usage Guide:

IPv6 type 0 route header allows the packet source node specify the transitional route node list that the packet will pass on its way to the destination node. These transitional nodes are not on the regular routes. The router/switch with RH0 handling function will transform the RH0 when receiving a packet containing RH0 and will send it to the next transitional node or the destination node. There is a DOS vulnerability in the design of IPv6 RH0, so users are not recommended to use this function unless for special purpose.

Examples:

Enable the IPv6 RH0 handling functions.

```
Switch(config)# ipv6 rthdr-type0 enable
```

17.2.28 interface tunnel

Command:

interface tunnel *<tnl-id>*

no interface tunnel *<tnl-id>*

Function:

Create/Delete tunnel.

Parameter:

Parameter <tnl-id> is tunnel No.

Command Mode:

Interface Configuration Mode.

Default:

None.

Usage Guide:

This command creates a virtual tunnel interface. Since there is not information such as specific tunnel mode and tunnel source, ***show ipv6 tunnel*** does not show the tunnel, enter tunnel mode after creating, under that model information such as tunnel source and destination can be specified. No command is to delete a tunnel.

Example:

Create tunnel 1.

```
Switch(Config)#interface tunnel 1
```

17.2.29 show ip traffic

Command:

show ip traffic

Function:

Display statistics for IP packets.

Command mode:

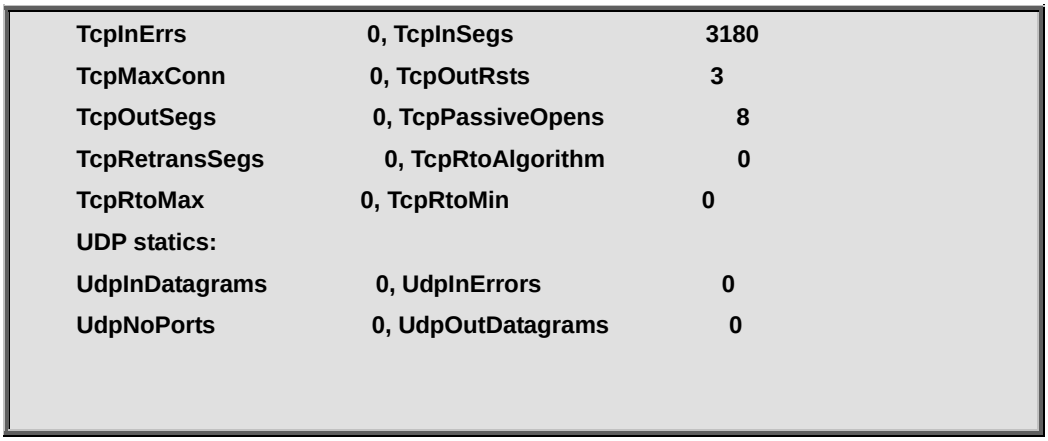
Admin Mode

Usage Guide:

Display statistics for IP, ICMP, TCP, UDP packets received/sent.

Example:

```
Switch#show ip traffic
    IP statistics:
    Rcvd:  3249810 total, 3180 local destination
       0 header errors, 0 address errors
       0 unknown protocol, 0 discards
    Frags:  0 reassembled, 0 timeouts
       0 fragment rcvd, 0 fragment dropped
       0 fragmented, 0 couldn't fragment, 0 fragment sent
    Sent:    0 generated, 3230439 forwarded
        0 dropped, 0 no route
    ICMP statistics:
    Rcvd:  0 total 0 errors 0 time exceeded
       0 redirects, 0 unreachable, 0 echo, 0 echo replies
       0 mask requests, 0 mask replies, 0 quench
       0 parameter, 0 timestamp, 0 timestamp replies
    Sent:    0 total 0 errors 0 time exceeded
       0 redirects, 0 unreachable, 0 echo, 0 echo replies
       0 mask requests, 0 mask replies, 0 quench
       0 parameter, 0 timestamp, 0 timestamp replies
    TCP statistics:
    TcpActiveOpens            0, TcpAttemptFails          0
    TcpCurrEstab              0, TcpEstabResets           0
```



Displayed information Explanation
IP statistics： IP packet statistics.
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics： ICMP packet statistics.
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench

0 parameter, 0 timestamp, 0 timestamp replies Statistics of total ICMP packets received and classified information
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies Statistics of total ICMP packets sent and classified information
TCP statistics: TCP packet statistics.
UDP statistics: UDP packet statistics.

17.2.30 show ipv6 interface

Command:

show ipv6 interface {brief|<*interface-name*>}

Function:

Show interface IPv6 parameters.

Parameter:

Parameter brief is the brief summarization of IPv6 status and configuration, and parameter interface-name is Layer 3 interface name.

Default:

None

Command Mode:

Admin Mode

Usage Guide:

If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.

Example:

```
Switch#show ipv6 interface Vlan1
    Vlan1 is up, line protocol is up, dev index is 2004
    Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
    IPv6 is enabled
    Link-local address(es):
    fe80::203:fff:fe00:10    PERMANENT
    Global unicast address(es):
    3001::1                                    subnet is 3001::1/64    PERMANENT
    Joined group address(es):
   ff02::1
   ff02::16
   ff02::2
   ff02::5
   ff02::6
   ff02::9
   ff02::d
   ff02::1:ff00:10
   ff02::1:ff00:1
   MTU is 1500 bytes
   ND DAD is enabled,      number of DAD attempts is 1
   ND managed_config_flag is unset
   ND other_config_flag is unset
   ND NS interval is 1 second(s)
   ND router advertisements is disabled
   ND RA min-interval is 200 second(s)
   ND RA max-interval is 600 second(s)
   ND RA hoplimit is 64
   ND RA lifetime is 1800 second(s)
   ND RA MTU is 0
   ND advertised reachable time is 0 millisecond(s)
   ND advertised retransmit time is 0 millisecond(s)
```

Displayed information Explanation
Vlan1 Layer 3 interface name

[up/up] Layer 3 interface status
dev index Internal index No.
fe80::203:fff:fe00:10 Automatically configured IPv6 address of Layer 3 interface
3001::1 Configured IPv6 address of Layer 3 interface

17.2.31 show ipv6 route

Command:

show ipv6 route [<*destination*>|<*destination* >|<*length*>| database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics]

Function:

Display IPv6 routing table.

Parameter:

<destination> is destination network address;

<destination >|<length> is destination network address plus prefix length;

connected is directly connected router;

static is static router;

rip is RIP router;

ospf is OSPF router;

bgp is BGP router;

isis is ISIS router;

kernel is kernel router;

statistics shows router number;

database is router database.

Default Situation:

None.

Command Mode:

Admin Mode.

Usage Guide:

show ipv6 route only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router, fib local shows the local router, statistics shows router statistics information.

Example:

```
Switch#show ipv6 route
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
```

```
C       ::/0        via ::,     tunnel3     256
S       2001:2::/32         via fe80::789,      Vlan2     1024
S       2001:2:3:4::/64         via fe80::123,      Vlan2     1024
O       2002:ca60:c801:1::/64       via ::,     Vlan1     1024
C       2002:ca60:c802:1::/64       via ::,     tunnel49      256
C       2003:1::/64         via ::,     Vlan4     256
C       2003:1::5efe:0:0/96         via ::,     tunnel26      256
S       2004:1:2:3::/64         via fe80:1::88,     Vlan2     1024
O       2006:1::/64         via ::,     Vlan1     1024
S       2008:1:2:3::/64         via fe80::250:baff:fef2:a4f4,     Vlan1     1024
C       2008:2005:5:8::/64          via ::,     Ethernet0     256
S       2009:1::/64         via fe80::250:baff:fef2:a4f4,     Vlan1     1024
C       2022:1::/64         via ::,     Ethernet0     256
O       3333:1:2:3::/64         via fe80::20c:ceff:fe13:eac1,     Vlan12      1024
C       3ffe:501:ffff:1::/64        via ::,     Vlan4     256
O       3ffe:501:ffff:100::/64          via ::,     Vlan5     1024
O       3ffe:3240:800d:1::/64           via ::,     Vlan1     1024
O       3ffe:3240:800d:2::/64           via ::,     Vlan2     1024
O       3ffe:3240:800d:10::/64          via ::,     Vlan12      1024
O       3ffe:3240:800d:20::/64          via fe80::20c:ceff:fe13:eac1,     Vlan12      1024
C       fe80::/64       via ::,     Vlan1     256
C       fe80::5efe:0:0/96           via ::,     tunnel26      256
C       ff00::/8        via ::,     Vlan1     256
```

Displayed information Explanation
IPv6 Routing Table IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info Abbreviation display sign of every entry
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024 The static router in FIB table, of which the destination network segment is 2002::/64, via means passing fe80::250:baff:fef2:a4f4 is the next hop, VLAN1 is the exit interface name, 1024 is router weight.

17.2.32 show ipv6 neighbors

Command:

show ipv6 neighbors[{vlan|ethernet|tunnel}*interface-number*| *interface-name* | address *<ipv6address>*]

Function:

Display neighbor table entry information.

Parameter:

Parameter **{vlan|ethernet|tunnel}*interface-number*|*interface-name*** specify the lookup based on interface. Parameter ***ipv6-address*** specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

Default Situation:

None

Command Mode:

Admin Mode

Usage Guide:

Example:

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0,
manage items 5
IPv6 Address                          Hardware Addr     Interface        Port
State
2002:ca60:c801:1:250:baff:fef2:a4f4   00-50-ba-f2-a4-f4   Vlan1          Ethernet1/2
reachable
3ffe:3240:800d:1::100                 00-30-4f-01-27-86   Vlan1          Ethernet1/3
reachable
3ffe:3240:800d:1::8888                00-02-01-00-00-00   Vlan1          Ethernet1/1
permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4   00-50-ba-f2-a4-f4   Vlan1          Ethernet1/4
reachable
3ffe:3240:800d:2::8888                00-02-01-00-01-01   Vlan2          Ethernet1/16
permanent
3ffe:3240:800d:2:203:fff:fefe:3045    00-30-4f-fe-30-45   Vlan2          Ethernet1/15
reachable
fe80::203:fff:fe01:2786               00-30-4f-01-27-86   Vlan1          Ethernet1/5
reachable
fe80::203:fff:fefe:3045               00-30-4f-fe-30-45   Vlan2          Ethernet1/17
reachable
fe80::20c:ceff:fe13:eac1              00-0c-ce-13-ea-c1   Vlan12         Ethernet1/20
reachable
fe80::250:baff:fef2:a4f4              00-50-ba-f2-a4-f4   Vlan1          Ethernet1/6
reachable
IPv6 neighbour table: 11 entries
```

Displayed information Explanation
IPv6 Addres Neighbor IPv6 address
Link-layer Addr. Neighbor MAC address
Interface Exit interface name
Port Exit interface name
State Neighbor status (reachable、statle、delay、probe、permanent、incomplete、unknow)

17.2.33 show ipv6 traffic

Command:

show ipv6 traffic

Function:

Display IPv6 transmission data packets statistics information.

Parameter:

None

Default:

None

Command Mode:

Admin Mode

Example:

```
Switch#show ipv6 traffic
IP statistics:
Rcvd:  90 total, 17 local destination
       0 header errors, 0 address errors
       0 unknown protocol, 13 discards
Frags: 0 reassembled, 0 timeouts
       0 fragment rcvd, 0 fragment dropped
       0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent:  110 generated, 0 forwarded
       0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
```


Displayed information Explanation
IP statistics IPv6 data report statistics
Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknown protocol, 13 discards IPv6 received packets statistics
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent IPv6 fragmenting statistics
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route IPv6 sent packets statistics

17.2.34 show ipv6 enable

Command:

show ipv6 enable

Function:

Display IPv6 transmission function on/off status.

Parameter:

None

Default:

None

Command Mode:

Admin Mode

Example:

Switch#show ipv6 enable

ipv6 enable has been on

Displayed information Explanation
ipv6 enable has been on IPv6 transmission switch is at on status

17.2.35 show ipv6 redirect

Command:

show ipv6 redirect

Function:

Display the state IPv6 redirect switch.

Parameters:

None.

Default:

None.

Command Mode:

Admin Mode.

Usage Guide:

This command can be used to check whether the IPv6 redirect function in the system is enabled.

Examples:

```
Switch# show ipv6 redirect
ipv6 redirect is disabled
```

17.2.36 show ipv6 tunnel

Command:

show ipv6 tunnel [<*tnl-id*>]

Function:

Display tunnel information.

Parameter:

Parameter ***<tnl-id>*** is tunnel No.

Default Situation:

None.

Command Mode:

Admin Mode.

Usage Guide:

If there is not tunnel number, then information of all tunnels are shown. If there is tunnel number, then the detailed information of specified tunnel is shown.

Example:

```
Switch#show ipv6 tunnel
name      mode      source          destination      nexthop
tunnel3    6to4     178.1.1.1
```

Displayed information Explanation
Name

Tunnel name
Mode Tunnel type
Source Tunnel source ipv4 address
Destination Tunnel destination ipv4 address
Nexthop Tunnel next hop (only applies to ISATAP tunnel)

17.2.37 description

Command:

description <*desc*>

no description

Function:

Configure the tunnel description. The no operation of this command will delete the tunnel description.

Parameters:

<desc> is the tunnel description, which is a string no longer than 31 characters, without any spaces or tab between characters.

Command Mode:

Tunnel Configuration Mode.

Default:

There is no tunnel description by default.

Usage Guide:

When there is more than one tunnel in the system, configuring description will help user with identifying the purposes of different tunnels.

Examples:

Set the tunnel description as toCernet2.

```
Switch(Config-if-Tunnel1)#description toCernet2
```

17.2.38 tunnel source

Command:

tunnel source {<*ipaddress*>|<*interface-name*>}

no tunnel source {*<ipaddress>*|*<interface-name>*}

Function:

Configure tunnel source.

Parameter:

<ipv4-daddress> is the ipv4 address of tunnel source.

Command Mode:

Tunnel Configuration Mode.

Default Situation:

None.

Usage Guide:

None.

Example:

Configure tunnel source IPv4 address 202.89.176.6.

```
Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6
```

17.2.39 tunnel destination

Command: .

tunnel destination <ipaddress>

no tunnel destination *<ipaddress>*

Function:

Configure tunnel destination.

Parameter:

<ipv4-daddress> is the ipv4 address of tunnel destination.

Command Mode:

Tunnel Configuration Mode.

Default Situation:

None.

Usage Guide:

None.

Example:

Configure tunnel destination 203.78.120.5.

```
Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5
```

17.2.40 tunnel nexthop

Command:

tunnel nexthop <*ipaddress*>

no tunnel nexthop <*ipaddress*>

Function:

Configure tunnel next hop.

Parameter:

<ipaddress> is the ipv4 address of tunnel next hop.

Command Mode:

Tunnel Configuration Mode.

Default Situation:

None.

Usage Guide:

This command is for ISATAP tunnel, other tunnels won't check the configuration of nexthop.

Example:

Configure tunnel next hop 178.99.156.8.

```
Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7
Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8
Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap
```

17.2.41 tunnel 6to4-relay

Command:

tunnel 6to4-relay <*ipdaddress*>

no tunnel 6to4-relay <*ipdaddress*>

Function:

Configure the 6to4 tunnel relay IPv4 address.

Parameters:

<ipdaddress>is the 6to4 tunnel relay IPv4 address.

Command Mode:

Tunnel Configuration Mode.

Default:

None.

Usage Guide:

This command is used to configure the 6to4 tunnel relay IPv4 address, which will not be checked

when configuring 6to4 tunnel relay. This relay IPv4 address will only be used when the packet uses default route with a destination address not starting with a prefix of 2002.

Examples:

Configure the 6to4 tunnel relay IPv4 address as 178.99.156.8.

```
Switch (Config-if-Tunnel1)#tunnel 6to4-relay 178.99.156.8
```

17.2.42 tunnel mode

Command:

tunnel mode ipv6ip [6to4 | isatap]

no tunnel mode ipv6ip [6to4 | isatap]

Function:

Configure Tunnel Mode.

Parameter:

None.

Command Mode:

Tunnel Configuration Mode.

Default:

None.

Usage Guide:

In configuring tunnel mode, only specifying ipv6ip indicates configuring tunnel. Ipv6ip 6to4 indicates it is 6to4 tunnel, ipv6ip isatap indicates it is ISATAP tunnel.

Example:

Configure tunnel mode.

```
1、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip
```

```
2、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4
```

```
3、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap
```

17.3 Commands for IP Route Aggregation

17.3.1 ip fib optimize

Command:

ip fib optimize

no ip fib optimize

Function:

Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

Default:

Optimized IP route aggregation algorithm is disabled by default.

Command mode:

Global Mode.

Usage Guide:

This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding a virtual default route to the chip segment route table reduces CPU load, it may introduce unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.

Example:

Disabling optimized IP route aggregation algorithm.

```
Switch(config)# no ip fib optimize
```

17.4 Commands for URPF

17.4.1 debug l4driver urpf

Command:

debug l4driver urpf {notice| warning| error}

no debug l4driver urpf {notice| warning| error}

Function:

Enable the URPF debug function to display error information if failures occur during the installation of URPF rules.

Command Mode:

Admin Mode

Parameters:

None

Usage Guide:

None

Example:

```
Switch#debug l4driver urpf error
```

17.4.2 ip urpf enable

Command:

ip urpf enable {loose | strict} {allow-default-route}

no ip urpf enable

Function:

Enable the URPF function on the port.

Parameters:

loose：the loose mode;

strict：the strict mode;

allow-default-route：allow the default route.

Command mode:

Port Mode

Default:

The URPF function is disabled on the port by default.

Usage Guide:

Users should specify the mode: loose or strict.

Example:

Switch(config)#interface ethernet 1/4
Switch(Config-If-Ethernet1/4)#ip urpf enable strict
Switch(Config-If-Ethernet1/4)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#ip urpf enable loose
Switch(Config-If-Ethernet1/5) #interface ethernet 1/6
Switch(Config-If-Ethernet1/6)#ip urpf enable loose allow-default-route
Switch(Config-If-Ethernet1/6)#interface ethernet 1/7
Switch(Config-If-Ethernet1/7)#ip urpf enable strict allow-default-route

17.4.3 show urpf rule ipv4 num

Command:

show urpf rule ipv4 num interface {ethernet IFNAME | IFNAME}

Function:

Display the number of IPv4 rules bonded to the port.

Parameters:

IFNAME: specify the port name.

Command Mode:

Admin and Configuration Mode

Usage Guide:

None

Examples:

Display the number of IPv4 rules bonded to the port Ethernet1/4.

```
Switch#show urpf rule ipv4 num interface ethernet 1/4
```

17.4.4 show urpf rule ipv6 num

Command:

show urpf rule ipv6 num interface {ethernet IFNAME | IFNAME}

Function:

Display the number of IPv6 rules bonded to the port.

Parameters:

IFNAME: specify the port name.

Command Mode:

Admin and Configuration Mode

Usage Guide:

None

Example:

Display the number of IPv6 rules bonded to the port Ethernet1/4.

```
Switch#show urpf rule ipv6 num interface ethernet 1/4
```

17.4.5 show urpf rule ipv4

Command:

show urpf rule ipv4 interface {ethernet IFNAME | IFNAME}

Function:

Display the details of IPv4 rules bonded to the port.

Parameters:

IFNAME: specify the port name.

Command Mode:

Admin and Configuration Mode

Usage Guide:

Display the currently distributed rules.

Examples:

Display the details of IPv4 rules bonded to the port Ethernet1/4.

```
Switch#show urpf rule ipv4 interface ethernet 1/4
```

17.4.6 show urpf rule ipv6

Command:

show urpf rule ipv6 interface {ethernet IFNAME | IFNAME}

Function:

Display the details of IPv6 rules bonded to the port.

Parameters:

IFNAME: specify the port name.

Command Mode:

Admin and Configuration Mode

Usage Guide:

Display the currently distributed rules.

Examples:

Display the details of IPv6 rules bonded to the port ethernet1/4.

```
Switch#show urpf rule ipv6 interface ethernet 1/4
```

17.4.7 show urpf

Command:

show urpf

Function:

Display which interfaces have been enabled with URPF function.

Command Mode:

Admin and Configuration Mode

Parameters:

None

Usage Guide:

None

Example:

```
Switch#show urpf
```

17.4.8 urpf enable

Command:

urpf enable

no urpf enable

Function:

Enable the global URPF function.

Parameters:

None

Command mode:

Global Mode

Default:

The URPF protocol module is disabled by default.

Usage Guide:

None

Example:

```
Switch(config)#urpf enable
```

17.5 Commands for ARP Configuration

17.5.1 arp

Command:

arp <*ip_address*> <*mac_address*> {interface [ethernet] <*portName*>}

no arp <*ip_address*>

Function:

Configures a static ARP entry; the "**no arp <*ip_address*>**" command deletes a ARP entry of the specified IP address.

Parameters:

<ip_address> is the IP address, at the same filed with interface address; ***<mac_address>*** is the MAC address; **ethernet** stands for Ethernet port; ***<portName>*** for the name of layer2 port.

Default:

No static ARP entry is set by default.

Command mode:

VLAN Interface Mode

Usage Guide:

Static ARP entries can be configured in the switch.

Example:

Configuring static ARP for interface VLAN1.

```
Switch(Config-if-Vlan1)#arp 1.1.1.1 00-30-4f-f0-12-34 eth 1/2
```

17.5.2 clear arp-cache

Command:

clear arp-cache

Function:

Clears ARP table.

Command mode:

Admin Mode

Usage Guide:

Clears the content of current ARP table, but it does not clear the current static ARP table.

Example:

```
Switch#clear arp-cache
```

17.5.3 clear arp traffic

Command:

clear arp traffic

Function:

Clear the statistic information of ARP messages of the switch. For box switches, this command will only clear statistics of APP messages received and sent from the current boardcard.

Command mode:

Admin Mode

Example:

```
Switch#clear arp traffic
```

17.5.4 debug arp

Command:

debug arp {receive|send|state}

no debug arp {receive|send|state}

Function:

Enables the ARP debugging function; the "**no debug arp {receive|send|state}**" command disables this debugging function.

Parameter:

receive the debugging-switch of receiving ARP packets of the switch; **send** the debugging-switch of sending ARP packets of the switch; **state** the debugging-switch of APR state changing of the switch.

Default:

ARP debug is disabled by default.

Command mode:

Admin Mode.

Usage Guide:

Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example:

Enabling ARP debugging.

```
Switch#debug arp receive
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
```

17.5.5 ip proxy-arp

Command:

ip proxy-arp

no ip proxy-arp

Function:

Enables proxy ARP for VLAN interface; the “no ip proxy-arp” command disables proxy ARP.

Default:

Proxy ARP is disabled by default.

Command mode:

VLAN Interface Mode

Usage Guide:

When an ARP request is received on the layer 3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, and the proxy ARP interface has been enabled, the interface will reply to the ARP with its own MAC address and forward the actual packets received. Enabling this function allows machines to physically be separated but in the same IP segment and communicate via the proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded if the destination is reachable.

Note: the ARP request matching default route will not use proxy.

Example:

Enabling proxy ARP for VLAN 1.

```
Switch(Config-if-Vlan1)#ip proxy-arp
```

17.5.6 l3 hashselect

Command:

l3 hashselect [<*crc16l*|*crc16u*|*crc32l*|*crc32u*|*lsb*>]

Function:

Set L3 table (hardware ARP table) HASH algorithm.

Parameters:

<crc16l|crc16u|crc32l|crc32u|lsb>is a specified HASH algorithm. The system default value is crc32u.

Command Mode:

Global Configuration Mode.

Usage Guide:

HASH algorithm is a fast searching algorithm. Setting that of L3 table will change the storage location and order of ARP entries in the hardware. This command is mainly used to solve the conflicts of ARP entries in the hardware table. When using the command to change the HASH algorithms of L3 table, the new HASH algorithm will take effect after the consumers save the configuration and restart system. The system will use the primary HASH algorithms before restart system. Since all HASH algorithms may have HASH crashes under certain circumstances, particular network configuration requires particular HASH algorithm. After repeated tests and verifications, the recommended order of the five HASH algorithms mentioned above is: crc32u ،crc32l ،crc16u ،crc16l. Generally speaking, lsb algorithm is not recommended.

When using this command to change the HASH algorithms of L3 table, users should make effective analysis of the network ARP configuration. That is why this command should uses under the guide of technicians from the vendor after they analyze the network ARP configuration.

Examples:

Set the HASH algorithm as crc32u.

```
Switch(Config-if-Vlan1)#l3 hashselect crc32u
```

17.5.7 show arp

Command:

show arp [<*ipaddress*>] [<*vlan-id*>] [<*hw-addr*>] [type {static | dynamic}] [count] [vrf word]

Function:

Displays the ARP table.

Parameters:

<ipaddress> is a specified IP address; ***<vlan-id>*** stands for the entry for the identifier of specified VLAN; ***<hw-addr>*** for entry of specified MAC address; **static** for static ARP entry; **dynamic** for dynamic ARP entry; **count** displays number of ARP entries; **word** is the specified vrf name.

Command mode:

Admin Mode

Usage Guide:

Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.

Example:

```
Switch#show arp
ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0
Address          Hardware Addr     Interface    Port           Flag
50.1.1.6         00-0a-eb-51-51-38 Vlan50       Ethernet1/11   Dynamic
50.1.1.9         00-00-00-00-00-09 Vlan50       Ethernet1/1    Static
150.1.1.2        00-00-58-fc-48-9f Vlan150      Ethernet1/4    Dynamic
```

Displayed information Explanation
Total arp items Total number of ARP entries.
Valid ARP entry number matching the filter conditions and attributing the legality states.
Matched ARP entry number matching the filter conditions.
Verifying ARP entry number at verifying again validity for ARP.
InCompleted ARP entry number have ARP request sent without ARP reply.
Failed ARP entry number at failed state.
None ARP entry number at begin-found state.
Address IP address of ARP entries.
Hardware Address MAC address of ARP entries.
Interface

Layer 3 interface corresponding to the ARP entry.
Port Physical (Layer2) port corresponding to the ARP entry.
Flag Describes whether ARP entry is dynamic or static.

17.5.8 show arp traffic

Command:

show arp traffic

Function:

Display the statistic information of ARP messages of the switch. For box switches, this command will only show statistics of APP messages received and sent from the current boardcard.

Command mode:

Admin and Config Mode

Usage Guide:

Display statistics information of received and sent APP messages.

Example:

```
Switch#show arp traffic
ARP statistics:
  Rcvd:   10 request, 5 response
  Sent:    5 request, 10 response
```

Chapter 18 Commands for ARP Scanning Prevention

18.1 anti-arpscan enable

Command:

anti-arpscan enable

no anti-arpscan enable

Function:

Globally enable ARP scanning prevention function; "**no anti-arpscan enable**" command globally disables ARP scanning prevention function.

Parameters:

None.

Default Settings:

Disable ARP scanning prevention function.

Command Mode:

Global configuration mode

User Guide:

When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example:

Enable the ARP scanning prevention function of the switch.

```
Switch(config)#anti-arpscan enable
```

18.2 anti-arpscan port-based threshold

Command:

anti-arpscan port-based threshold *<threshold-value>*

no anti-arpscan port-based threshold

Function:

Set the threshold of received messages of the port-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the port will be closed. The unit is packet/second. The "no anti-arpscan port-based threshold" command will reset the default value, 10 packets/second.

Parameters:

rate threshold, ranging from 2 to 200.

Default Settings:

10 packets /second.

Command Mode:

Global Configuration Mode.

User Guide:

the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example:

Set the threshold of port-based ARP scanning prevention as 10 packets /second.

```
Switch(config)#anti-arpscan port-based threshold 10
```

18.3 anti-arpscan ip-based threshold

Command:

anti-arpscan ip-based threshold <*threshold-value*>

no anti-arpscan ip-based threshold

Function:

Set the threshold of received messages of the IP-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the IP messages from this IP will be blocked. The unit is packet/second. The “no anti-arpscan ip-based threshold” command will reset the default value, 3 packets/second.

Parameters:

rate threshold, ranging from 1 to 200.

Default Settings:

3 packets/second.

Command Mode:

Global configuration mode

User Guide:

The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example:

Set the threshold of IP-based ARP scanning prevention as 6 packets/second.

```
Switch(config)#anti-arpscan ip-based threshold 6
```

18.4 anti-arpscan trust

Command:

anti-arpscan trust [port | supertrust-port]

no anti-arpscan trust [port | supertrust-port]

Function:

Configure a port as a trusted port or a super trusted port;” **no anti-arpscan trust <port | supertrust-port>**”command will reset the port as an untrusted port.

Parameters:

None.

Default Settings:

By default all the ports are non- trustful.

Command Mode:

Port configuration mode

User Guide:

If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super non- trustful port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.

When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example:

Set port ethernet 4/5 of the switch as a trusted port.

```
Switch(config)#in e4/5
```

```
Switch(Config-If-Ethernet4/5)# anti-arpscan trust port
```

18.5 anti-arpscan trust ip

Command:

anti-arpscan trust ip <*ip-address*> [<*netmask*>]

no anti-arpscan trust ip <*ip-address*> [<*netmask*>]

Function:

Configure trusted IP;" **no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**"command reset the IP to non-trustful IP.

Parameters:

<*ip-address*>: Configure trusted IP address; **<*netmask*>:** Net mask of the IP.

Default Settings:

By default all the IP are non-trustful. Default mask is 255.255.255.255

Command Mode:

Global configuration mode

User Guide:

If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.

Example:

Set 192.168.1.0/24 as trusted IP.

```
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
```

18.6 anti-arpscan recovery enable

Command:

anti-arpscan recovery enable

no anti-arpscan recovery enable

Function:

Enable the automatic recovery function, "**no anti-arpscan recovery enable**" command will disable the function.

Parameters:

None

Default Settings:

Enable the automatic recovery function

Command Mode:

Global configuration mode

User Guide:

If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.

Example:

Enable the automatic recovery function of the switch.

```
Switch(config)#anti-arpscan recovery enable
```

18.7 anti-arpscan recovery time

Command:

anti-arpscan recovery time <*seconds*>

no anti-arpscan recovery time

Function:

Configure automatic recovery time; "**no anti-arpscan recovery time**" command resets the automatic recovery time to default value.

Parameters:

Automatic recovery time, in second ranging from 5 to 86400.

Default Settings:

300 seconds.

Command Mode:

Global configuration mode

User Guide:

Automatic recovery function should be enabled first.

Example:

Set the automatic recovery time as 3600 seconds.

```
Switch(config)#anti-arpscan recovery time 3600
```

18.8 anti-arpscan log enable

Command:

anti-arpscan log enable

no anti-arpscan log enable

Function:

Enable ARP scanning prevention log function; "**no anti-arpscan log enable**" command will disable this function.

Parameters:

None.

Default Settings:

Enable ARP scanning prevention log function.

Command Mode:

Global configuration mode

User Guide:

After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is "Warning".

Example:

Enable ARP scanning prevention log function of the switch.

```
Switch(config)#anti-arpscan log enable
```

18.9 anti-arpscan trap enable

Command:

anti-arpscan trap enable

no anti-arpscan trap enable

Function:

Enable ARP scanning prevention SNMP Trap function; "**no anti-arpscan trap enable**" command disable ARP scanning prevention SNMP Trap function.

Parameters:

None.

Default Settings:

Disable ARP scanning prevention SNMP Trap function.

Command Mode:

Global configuration mode

User Guide:

After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.

Example:

Enable ARP scanning prevention SNMP Trap function of the switch.

```
Switch(config)#anti-arpscan trap enable
```

18.10 show anti-arpscan

Command:

show anti-arpscan [trust [ip | port | supertrust-port] |prohibited [ip | port]]

Function:

Display the operation information of ARP scanning prevention function.

Parameters:

None.

Default Settings:

Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Command Mode:

Admin Mode

User Guide:

Use "**show anti-arpscan trust port**" if users only want to check trusted ports. The reset follow the same rule.

Example:

Check the operating state of ARP scanning prevention function after enabling it.

```
Switch(config)#show anti-arpscan
Total port: 28
Name            Port-property   beShut   shutTime(seconds)
Ethernet1/1       untrust         N        0
Ethernet1/2       untrust         N        0
Ethernet1/3       untrust         N        0
Ethernet1/4       untrust         N        0
Ethernet1/5       untrust         N        0
Ethernet1/6       untrust         N        0
Ethernet1/7       untrust         N        0
Ethernet1/8       untrust         N        0
Ethernet1/9       untrust         N        0
Ethernet1/10      untrust         N        0
Ethernet1/11      untrust         N        0
Ethernet1/12      untrust         N        0
Ethernet4/1       untrust         N        0
Ethernet4/2       untrust         N        0
Ethernet4/3       untrust         N        0
Ethernet4/4       trust           N        0
Ethernet4/5       untrust         N        0
Ethernet4/6       supertrust      N        0
Ethernet4/7       untrust         Y        30
Ethernet4/8       trust           N        0
Ethernet4/9       untrust         N        0
Ethernet4/10      untrust         N        0
Ethernet4/11      untrust         N        0
```

```
Ethernet4/12    untrust    N    0
Ethernet4/13    untrust    N    0
Ethernet4/14    untrust    N    0
Ethernet4/15    untrust    N    0
Ethernet4/16    untrust    N    0
Ethernet4/17    untrust    N    0
Ethernet4/18    untrust    N    0
Ethernet4/19    untrust    N    0
Ethernet4/20    untrust    N    0
Ethernet4/21    untrust    N    0
Ethernet4/22    untrust    N    0
Ethernet4/23    untrust    N    0
Ethernet4/24    untrust    N    0

Prohibited IP:
IP              shutTime(seconds)
1.1.1.2         132

Trust IP:
192.168.99.5    255.255.255.255
192.168.99.6    255.255.255.255
```

18.11 debug anti-arpscan

Command:

debug anti-arpscan [port | ip]

no debug anti-arpscan [port | ip]

Function:

Enable the debug switch of ARP scanning prevention; "**no debug anti-arpscan [port | ip]**" command disables the switch.

Parameters:

None.

Default Settings:

Disable the debug switch of ARP scanning prevention

Command Mode:

Admin Mode

User Guide:

After enabling debug switch of ARP scanning prevention users can check corresponding debug information or enable the port-based or IP-based debug switch separately whenever a port is closed by ARP scanning prevention or recovered automatically, and whenever IP t is closed or recovered .

Example:

Enable the debug function for ARP scanning prevention of the switch.

```
Switch(config)#debug anti-arpscan
```

Chapter 19 Commands for Preventing ARP, ND Spoofing

19.1 ip arp-security updateprotect

Command:

ip arp-security updateprotect

no ip arp-security updateprotect

Function:

Forbid ARP table automatic update. The "**no ip arp-security updateprotect**" command re-enables ARP table automatic update.

Parameter:

None.

Default:

ARP table automatic update.

Command Mode:

Global Mode/ Interface configuration.

User Guide:

Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be droped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.

Example:

Switch(Config-if-Vlan1)#ip arp-security updateprotect.
Switch(config)#ip arp-security updateprotect.

19.2 ipv6 nd-security updateprotect

Command:

ipv6 nd-security updateprotect

no ipv6 nd-security updateprotect

Function:

Forbid ND automatic update function of IPv6 Version, the "**no ipv6 nd-security updateprotect**" command re-enables ND automatic update function.

Parameter:

None

Default:

ND update normally.

Command Mode:

Global Mode/ Interface configuration

User Guide:

Forbid ND table automatic update, the ND packets conflicting with current ND item (e.g. with same IP but different MAC or port) will be droped, the others will be received to update aging timer or create a new item; so, the current ND item keep unchanged and the new item can still be learned.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect
```

```
Switch(config)#ipv6 nd -security updateprotect
```

19.3 ip arp-security learnprotect

Command:

ip arp-security learnprotect

no ip arp-security learnprotect

Function:

Forbid ARP learning function of IPv4 Version, the "**no ip arp-security learnprotect**" command re-enables ARP learning function.

Parameter:

None.

Default:

ARP learning enabled.

Command Mode:

Global Mode/ Interface Configuration.

Usage Guide:

This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example:

```
Switch(Config-if-Vlan1)# ip arp-security learnprotect
```

```
Switch(config)# ip arp-security learnprotect
```

19.4 ipv6 nd-security learnprotect

Command:

ipv6 nd-security learnprotect

no ipv6 nd-security learnprotect

Function:

Forbid ND learning function of IPv6 Version, the "**no ipv6 nd-security learnprotect**" command re-enables ND learning function.

Parameter:

None.

Default:

ND learning enabled.

Command Mode:

Global Mode/ Interface Configuration.

Usage Guide:

This command is for preventing the automatic learning and updating of ND. Unlike ip nd-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect
```

```
Switch(config)#ipv6 nd -security learnprotect
```

19.5 ip arp-security convert

Command:

ip arp-security convert

Function:

Change all of dynamic ARP to static ARP.

Parameter:

None

Command Mode:

Global Mode/ Interface configuration

Usage Guide:

This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.

Example:

```
Switch(Config-if-Vlan1)#ip arp -security convert
```

```
Switch(config)#ip arp -security convert
```

19.6 ipv6 nd-security convert

Command:

ipv6 nd-security convert

Function:

Change all of dynamic ND to static ND.

Parameter:

None

Command Mode:

Global Mode/ Interface Configuration

Usage Guide:

This command will convert the dynamic ND entries to static ones, which, in combination with disabling automatic learning, can prevent ND binding. Once implemented, this command will lose its effect.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security convert
```

```
Switch(config)#ipv6 nd -security conver
```

19.7 clear ip arp dynamic

Command:

clear ip arp dynamic

Function:

Clear all of dynamic ARP on interface.

Parameter:

None

Command Mode:

Interface Configuration

Usage Guide:

This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.

Example:

```
Switch(Config-if-Vlan1)#clear ip arp dynamic
```

19.8 clear ipv6 nd dynamic

Command:

clear ipv6 nd dynamic

Function:

Clear all of dynamic ND on interface.

Parameter:

None

Command mode:

Interface Configuration

Usage Guide:

This command will clear dynamic entries before binding ND. Once implemented, this command will lose its effect.

Example:

```
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic
```

Chapter 20 Command for ARP GUARD

20.1 arp-guard ip

Command:

arp-guard ip <addr>

no arp-guard ip <addr>

Function:

Add a ARP GUARD address, the no command deletes ARP GUARD address.

Parameters:

<addr> is the protected IP address, in dotted decimal notation.

Default:

There is no ARP GUARD address by default.

Command Mode:

Port configuration mode

Usage Guide:

After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP messagse match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.

Example:

Configure the ARP GUARD address on port ethernet1/1 as 100.1.1.1.

switch(config)#interface ethernet1/1
switch(Config-If-Ethernet 1/1)#arp-guard ip 100.1.1.1

Delete the ARP GUARD address on port ethernet1/1 as 100.1.1.1.

switch(config)#interface ethernet1/1
switch(Config-If-Ethernet 1/1)#no arp-guard ip 100.1.1.1

Chapter 21 Command for ARP Local Proxy

21.1 ip local proxy-arp

Command:

ip local proxy-arp

no ip local proxy-arp

Function:

Enable/disable the local ARP Proxy function of a specified interface.

Parameters:

None.

Default Settings:

This function is disabled on all interfaces by default.

Command Mode:

Interface VLAN Mode.

User Guide:

This function is disabled on all interfaces by default, and differs from the original proxy-arp in that this function acts as an ARP Proxy inside the same layer-3 interface and thus directs the layer-3 forwarding of the switch.

Example:

Enable the local ARP Proxy function of interface VLAN1.

```
Switch(Config-if-Vlan1)# ip local proxy-arp
```

Chapter 22 Commands for Gratuitous ARP Configuration

22.1 ip gratuitous-arp

Command:

ip gratuitous-arp [<*interval-time*>]

no ip gratuitous-arp

Function:

To enabled gratuitous ARP, and specify update interval for gratuitous ARP. The no form of this command will disable the gratuitous ARP configuration.

Parameters:

<interval-time> is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.

Command Mode:

Global Configuration Mode and Interface Configuration Mode.

Default:

Gratuitous ARP is disabled by default.

Usage Guide:

When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.

Example:

1.To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.

```
Switch>enable
Switch#config
Switch(config)#ip gratuitous-arp 400
```

2.To enable gratuitous ARP for interface VLAN 10 and set the update interval to be 350 seconds.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

22.2 show ip gratuitous-arp

Command:

show ip gratuitous-arp [interface vlan <*vlan-id*>]

Function:

To display configuration information about gratuitous ARP.

Parameters:

<vlan-id> is the VLAN ID. The valid range for <*vlan-id*> is between 1 and 4094.

Command Mode:

All the Configuration Modes.

Usage Guide:

In all the configuration modes, the command **show ip gratuitous arp** will display information about the gratuitous ARP configuration in global and interface configuration mode. The command **show ip gratuitous-arp interface vlan *<vlan-id>*** will display information about the gratuitous ARP configuration about the specified VLAN interface.

Example:

1.To display information about gratuitous ARP configuration in both global and interface configuration modes.

```
Switch#show ip gratuitous-arp
Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:
Name            Interval-Time(seconds)
Vlan1           400
Vlan10          350
```

2.To display gratuitous ARP configuration information about interface VLAN 10.

```
Switch#show ip gratuitous-arp interface vlan 10
Gratuitous ARP send interface Vlan10 information:
Name            Interval-Time(seconds)
Vlan10          350
```

Chapter 23 Commands for ND Snooping

23.1 clear ipv6 nd snooping binding

Command:

clear ipv6 nd snooping binding [<*interface-name*>]

Function:

Clear all dynamic binding of ND Snooping.

Parameter:

<interface-name> the name of an ethernet port.

Default:

None.

Command mode:

Admin Mode.

Usage Guide:

Clear all ND Snooping binding table or binding entries of a port, the entries of the corresponding FFP hardware drive will also be cleared.

Example:

Switch(config)#ipv6 nd snooping enable
Switch# clear ipv6 nd snooping binding

23.2 debug ipv6 nd snooping

Command:

debug ipv6 nd snooping {packet | event | binding}

no debug ipv6 nd snooping {packet | event | binding}

Function:

Open/close the debug of ND Snooping.

Parameter:

packet shows debug information of received and sent ND packets, **event** shows debug information that ND snooping processes the packets and the timer event, **binding** shows the debug information of ND Snooping managing the binding table.

Default:

Disable the debug information.

Command mode:

Port Mode.

Usage Guide:

Open the debug information switch of ND Snooping.

Example:

Show the debug information of ND Snooping.

Switch#debug ipv6 nd snooping packet

```
Receive packet, smac 00-21-27-aa-0f-46, dmac 00-30-4f-00-de-01,
saddr fe80::221:27ff:feaa:f46, daddr 2001::1,
interface Ethernet1/17(portID 0x1000011), vid 1, length 90,
type 135, opcode 0, target address 2001::1
```

23.3 ipv6 nd snooping enable (Global mode)

Command:

ipv6 nd snooping enable

no ipv6 nd snooping enable

Function:

Enable/disable the monitoring function of ND Snooping globally.

Parameter:

None.

Command mode:

Global Mode.

Default:

Disable the global function of ND Snooping.

Usage Guide:

Only after ND Snooping enabled globally, the port configuration of ND Snooping is allowed, NA/NS packets of all ports are not forwarded, but are copied to cpu. After being processed by ND Snooping, these packets are forwarded according to the set rules.

Example:

Enable the ND Snooping globally.

```
Switch(config)#ipv6 enable
```

```
Switch(config)#ipv6 nd snooping enable
```

23.4 ipv6 nd snooping mac-binding-limit

Command:

ipv6 nd snooping mac-binding-limit <*number*>

no ipv6 nd snooping mac-binding-limit

Function:

Configure the max number of IPv6 addresses that can be bound to the same MAC address.

Parameter:

<number> is the max value. It only includes the dynamic binding number, the corresponding static binding number is not limited, the range from 1 to 10.

Default:

10.

Command mode:

Global Mode.

Usage Guide:

a) After receiving this configuration command, set globally the max number of dynamic binding which relate to the same MAC address.

b) Account the binding value which corresponds with each MAC address globally. If the corresponding dynamic binding number of one MAC address exceeds the configuration value, then delete some dynamic binding which have a high age until the number of the dynamic binding equals this configuration value, and stop the binding corresponding with this MAC address. If the numberr of binding is less than the configuration value, the new dynamic binding can still be created.

Example:

Set the max number of the corresponding dynamic binding for the same MAC address.

```
Switch(config)#ipv6 nd snooping enable
Switch(config)# ipv6 nd snooping mac-binding-limit 10
```

23.5 ipv6 nd snooping max-dad-delay

Command:

ipv6 nd snooping max-dad-delay <*max-dad-delay*>

no ipv6 nd snooping max-dad-delay

Function:

Set the lifetime of SAC_START state for a binding.

Parameter:

<*max-dad-delay*> is the lifetime of SAC_START state, the range from 1 to 10, the unit is second.

Command mode:

Global Mode.

Default:

SAC_START state binds the lifetime as 1 second.

Usage Guide:

Reset the binding lifetime of SAC_START state as <*max-dad-delay*> or 1 second.

Example:

Configure the lifetime as 10 seconds.

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-delay 10
```

23.6 ipv6 nd snooping max-dad-prepare-delay

Command:

ipv6 nd snooping max-dad-prepare-delay <*max-dad-prepare-delay*>

no ipv6 nd snooping max-dad-prepare-delay

Function:

Set the lifetime of SAC_QUERY state for a binding.

Parameter:

<max-dad-prepare-delay> is the lifetime of SAC_QUERY state, the range from 1 to 10, the unit is second.

Command mode:

Global Mode.

Default:

SAC_QUERY state binds the lifetime as half a second.

Usage Guide:

Reset the binding lifetime of SAC_QUERY state as <*max-dad-prepare-delay*> or half a second.

Example:

Configure the lifetime as 10 seconds.

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-prepare-delay 10
```

23.7 ipv6 nd snooping max-sac-lifetime

Command:

ipv6 nd snooping max-sac-lifetime <*max-sac-lifetime*>

no ipv6 nd snooping max-sac-lifetime

Function:

Set the lifetime of SAC_BOUND state for a binding.

Parameter:

<max-sac-lifetime> is the lifetime of SAC_BOUND state, the range from 1 to 31536000, the unit is second.

Default Configuration:

SAC_BOUND state binds the lifetime as 2 hours (7200 seconds).

Command mode:

Global Mode.

Default:

SAC_BOUND state binds the lifetime as 2 hours. (7200 seconds)

Usage Guide:

Change the lifetime of SAC_BOUND state.

Example:

Configure the lifetime as 36000 seconds.

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-sac-lifetime 36000
```

23.8 ipv6 nd snooping policy

Command:

ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address}

no ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address}

Function:

Configure the dynamic binding policy of ND Snooping addresses.

Parameter:

bind-eui64-address means only the address of the global unicast EUI-64 is bound, bind-non-eui64-address means the global unicast address of non EUI-64 is bound, default means the global unicast address is bound.

Command mode:

Global Mode.

Default:

Bind any global unicast addresses by default.

Usage Guide:

After the policy is configured, only bind the IPv6 addresses which are specified by the policy, a message is displayed for a non policy specifies the global unicast address to report the conflict.

Example:

Configure binding the global unicast EUI-64.

Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping policy bind-eui64-address

23.9 ipv6 nd snooping port-binding-limit

Command:

ipv6 nd snooping port-binding-limit <*binding-number*>

no ipv6 nd snooping port-binding-limit

Function:

Configure the binding number of the port. This binding number only limits the dynamic binding number of the port, but do not limit the number of the static binding.

Parameter:

binding-limit is the max number which can be bound for each port, the range from 1 to 100.

Command mode:

Port Mode.

Default:

100

Usage Guide:

a) After receiving this configuration command, set the max value of the dynamic binding for this port.

b) Check the dynamic binding of this port and account the number of the dynamic binding. If the number exceeds this configuration value, then delete some dynamic binding which have a high

age until the number of the dynamic binding equals this configuration value, and stop creating new dynamic binding of this port. If the number of the dynamic binding is less than this configuration value, new dynamic binding can still be created.

Example:

Configure the number which can be bound by the port.

```
Switch(config)#ipv6 nd snooping enable
```

```
Switch(config-if-ethernet1/1)#ipv6 nd snooping port-binding-limit 100
```

23.10 ipv6 nd snooping static-binding

Command:

ipv6 nd snooping static-binding <ipv6-address> hardware-address <hardware-address> interface <interface-name >

no ipv6 nd snooping static-binding <ipv6-address>

Function:

Add a static binding.

Parameter:

ipv6-address can bind the global unicast address only, can not bind the link local address , the unspecific address and the loopback address, **hardware-address** is the MAC address of IEEE802 hardware, **interface-name** is the corresponding port ID.

Command mode:

Global Mode.

Default:

None.

Usage Guide:

1.Check the configured IPv6 addresses, if the configured addresses are the multicast address of the nodes, the local address of the link, the unspecific address and the loopback address, then show the error information and return.

2.According to the IPv6 address and the MAC address of the configuration command to check the static binding table. If the IPv6 address binding exists, then give the binding information of this IPv6 address and return. If there is no IPv6 address binding, then create new static binding. If ND Snooping has been enabled in the binding port, then send the binding entries to FFP hardware drive.

3.Checking the dynamic binding table, if exist the dynamic binding for matching the static binding completely, then delete this dynamic binding and keep the entries in FFP hardware drive. If exist the binding corresponding with the IPv6 address, and the anchor information is different, then delete this dynamic binding and the entries in FFP hardware drive.

Example:

Add a new type of the binding table in the static binding table.

interface ethernet1/1

```
Switch(config)#ipv6 nd snooping enable
```

```
Switch(config)#ipv6 nd snooping static-binding 2001::2:1 hardware-address 00-11-22-33-44-55
interface ethernet1/1
```

23.11 ipv6 nd snooping trust

Command:

ipv6 nd snooping trust

no ipv6 nd snooping trust

Function:

Set the trust port of the switch.

Parameter:

None.

Command mode:

Port Mode.

Default:

un-trusted port.

Usage Guide:

This command sets a port or a group of ports as the trust port and deletes all dynamic binding corresponding with the port or ports, stop creating new binding of port or ports, and accessing of packets is also allowed.

Example:

Set a port or a group of ports as the trust ports.

```
Switch(config)#interface ethernet 1
```

```
Swithc(config-if-ethernet1/1)# ipv6 nd snooping trust
```

23.12 ipv6 nd snooping user-control

Command:

ipv6 nd snooping user-control

no ipv6 nd snooping user-control

Function:

Enable the control function of the ports for ND Snooping.

Parameter:

None.

Command mode:

Port Mode.

Default:

Disable the control function of ND Snooping.

Usage Guide:

After the control function of ND Snooping is disabled, clear all FFP drive entries which are sent by ND Snooping for this port, but the binding information is not deleted.

Example:

Configure ND Snooping function on the port.

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#interface ethernet 1
Swithc(config-if-ethernet1/1)# ipv6 nd snooping user-control
```

23.13 show ipv6 nd snooping

Command:

show ipv6 nd snooping [*<interface-name>*]

Function:

Show the configuration and the binding information of ND Snooping.

Parameter:

<interface-name> is the layer 2 port name which will be shown.

Default:

None.

Command mode:

Admin Mode.

Usage Guide:

Show the global configuration and all binding information of ND Snooping, or the configuration and the binding information of the port.

Example:

Show the configuration and the binding information of ND Snooping.

```
Switch#show ipv6 nd snooping
NDP Snooping is enabled
NDP snooping binding count 1, static binding 0
 MAC                IPv6 address                 interface       vlan ID   State
00-19-ef-d1-23-a4  2001::219:e0ff:fe3f:d183     Ethernet1/27       1    SAC_BOUND
```

23.14 show ipv6 nd snooping mac-binding

Command:

show ipv6 nd snooping mac-binding [hardware-address]

Function:

Show ND Snooping binding according to MAC address.

Parameter:

hardware-address is the MAC address of IEEE802.1 hardware.

Default:

Show the binding information for corresponding to all MAC addresses.

Command mode:

Global Mode.

Usage Guide:

1.If specify the MAC address, then show the information of the static binding and the dynamic binding corresponding with this MAC address.

2.If do not specify the MAC address, then show the information of the static binding and the dynamic binding corresponding with all MAC address.

Example:

Show the IPv6 binding information for corresponding with MAC address.
Switch#show ipv6 nd snooping mac-binding 00-19-ef-d1-23-a4 NDP Snooping is enabled NDP snooping binding count 2, static binding 0 MAC IPv6 address interface vlan ID State 00-19-ef-d1-23-a4 2001::219:e0ff:fe3f:d183 Ethernet1/27 1 SAC_BOUND 00-19-ef-d1-23-a4 FE80::219:e0ff:fe3f:d183 Ethernet1/27 1 SAC_BOUND

Chapter 24 Commands for DHCP

24.1 Commands for DHCP Server Configuration

24.1.1 bootfile

Command:

bootfile <*filename*>

no bootfile

Function:

Sets the file name for DHCP client to import on boot up; the "**no bootfile** "command deletes this setting.

Parameters:

<filename> is the name of the file to be imported, up to 255 characters are allowed.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the "next sever".

Example:

The path and filename for the file to be imported is "c:\temp\nos.img"

```
Switch(dhcp-1-config)#bootfile c:\temp\nos.img
```

Related Command:

next-server

24.1.2 clear ip dhcp binding

Command:

clear ip dhcp binding {<*address*> | all}

Function:

Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameters:

<address> is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.

Command mode:

Admin Mode.

Usage Guide:

"**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool

will be reallocated.

Example:

Removing all IP-hardware address binding records.

```
Switch#clear ip dhcp binding all
```

Related Command:

show ip dhcp binding

24.1.3 clear ip dhcp conflict

Command:

clear ip dhcp conflict {*<address>* | all }

Function:

Deletes an address present in the address conflict log.

Parameters:

<address> is the IP address that has a conflict record;

all stands for all addresses that have conflict records.

Command mode:

Admin Mode.

Usage Guide:

"**show ip dhcp conflict**" command can be used to check which IP addresses are conflicting for use. The **"clear ip dhcp conflict"** command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.

Example:

The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.

```
Switch#clear ip dhcp conflict 10.1.128.160
```

Related Command:

ip dhcp conflict logging, show ip dhcp conflict

24.1.4 clear ip dhcp server statistics

Command:

clear ip dhcp server statistics

Function:

Deletes the statistics for DHCP server, clears the DHCP server count.

Parameters:

None

Command mode:

Admin Mode.

Usage Guide:

DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all

information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.

Example:

Clearing the count for DHCP server.

```
Switch#clear ip dhcp server statistics
```

Related Command:

show ip dhcp server statistics

24.1.5 client-identifier

Command:

client-identifier <*unique-identifier*>

no client-identifier

Function:

Specifies the unique ID of the user when binding an address manually; the "**no client-identifier**" command deletes the identifier.

Parameters:

<unique-identifier> is the user identifier, in dotted Hex format.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

This command is used with "host" when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in "host" command to the client.

Example:

Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

```
Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12
```

```
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related Command:

Host

24.1.6 client-name

Command:

client-name <*name*>

no client-name

Function:

Specifies the username when binding addresses manually; the "**no client-name**" command deletes the username.

Parameters:

<name> is the name of the user, up to 255 characters are allowed.

Command Mode:

DHCP Address Pool Mode

Default:

None

Usage Guide:

Configure a username for the manual binding device, domain should not be included when configuring username.

Example:

Giving the user, with unique id of 00-10-5a-60-af-12, a username of "network".

```
Switch(dhcp-1-config)#client-name network
```

24.1.7 debug ip dhcp server

Command:

debug ip dhcp server { events | linkage | packets }

no debug ip dhcp server { events | linkage | packets }

Function:

Enables DHCP server debug information: the "**no debug ip dhcp server { events | linkage | packets }"** command disables the debug information for DHCP server**.**

Default:

Debug information is disabled by default.

Command mode:

Admin Mode.

24.1.8 default-router

Command:

default-router <*address1*>[<*address2*>[…<*address8*>]]

no default-router

Function:

Configures default gateway(s) for DHCP clients; the "**no default-router**" command deletes the default gateway.

Parameters:

<address1>…<address8> are IP addresses, in decimal format.

Default:

No default gateway is configured for DHCP clients by default.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.

Example:

Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

```
Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100
```

24.1.9 dns-server

Command:

dns-server <*address1*>[<*address2*>[...<*address8*>]]

no dns-server

Function:

Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameters:

<address1>...<address8> are IP addresses, in decimal format.

Default:

No DNS server is configured for DHCP clients by default.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.

Example:

Set 10.1.128.3 as the DNS server address for DHCP clients.

```
Switch(dhcp-1-config)#dns-server 10.1.128.3
```

24.1.10 domain-name

Command:

domain-name <*domain*>

no domain-name

Function:

Configures the Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameters:

<domain> is the domain name, up to 255 characters are allowed.

Command Mode:

DHCP Address Pool Mode

Default:

None

Usage Guide:

Specifies a domain name for the client.

Example:

Specifying “digitalchina.com.cn" as the DHCP clients’ domain name.

```
Switch(dhcp-1-config)#domain-name digitalchina.com.cn
```

24.1.11 hardware-address

Command:

hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}]

no hardware-address

Function:

Specifies the hardware address of the user when binding address manually; the “**no hardware-address**” command deletes the setting.

Parameters:

<hardware-address> is the hardware address in Hex; **Ethernet | IEEE802** is the Ethernet protocol type, ***<type-number>*** should be the RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.

Default:

The default protocol type is Ethernet,

Command Mode:

DHCP Address Pool Mode

Usage Guide:

This command is used with the “host” when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example:

Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.

```
Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04
```

```
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related Command:

Host

24.1.12 host

Command:

host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function:

Specifies the IP address to be assigned to the user when binding addresses manually; the "**no host**" command deletes the IP address.

Parameters:

<address> is the IP address in decimal format;

<mask> is the subnet mask in decimal format;

<prefix-length> means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".

Command Mode:

DHCP Address Pool Mode

Default:

None

Usage Guide:

If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example:

Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

```
Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related command:

hardware-address, client-identifier

24.1.13 ip dhcp conflict logging

Command:

ip dhcp conflict logging

no ip dhcp conflict logging

Function:

Enables logging for address conflicts detected by the DHCP server; the "**no ip dhcp conflict logging"** command disables the logging.

Default:

Logging for address conflict is enabled by default.

Command mode:

Global Mode

Usage Guide:

When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.

Example:

Disable logging for DHCP server.

```
Switch(config)#no ip dhcp conflict logging
```

Related Command:

clear ip dhcp conflict

24.1.14 ip dhcp excluded-address

Command:

ip dhcp excluded-address <*low-address*> [<*high-address*>]

no ip dhcp excluded-address <*low-address*> [<*high-address*>]

Function:

Specifies addresses excluding from dynamic assignment; the "**no ip dhcp excluded-address <*low-address*> [<*high-address*>]**" command cancels the setting.

Parameters:

<*low-address*> is the starting IP address,

[<*high-address*>] is the ending IP address.

Default:

Only individual address is excluded by default.

Command mode:

Global Mode

Usage Guide:

This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.

Example:

Reserving addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.

```
Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10
```

24.1.15 ip dhcp pool

Command:

ip dhcp pool <*name*>

no ip dhcp pool <*name*>

Function:

Configures a DHCP address pool and enter the pool mode; the "**no ip dhcp pool <*name*>**"command deletes the specified address pool.

Parameters:

<name> is the address pool name, up to 32 characters are allowed.

Command mode:

Global Mode

Usage Guide:

This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.

Example:

Defining an address pool named “1”.

```
Switch(config)#ip dhcp pool 1
Switch(dhcp-1-config)#
```

24.1.16 ip dhcp conflict ping-detection enable

Command:

ip dhcp conflict ping-detection enable

no ip dhcp conflict ping-detection enable

Function:

Enable Ping-detection of conflict on DHCP server; the no operation of this command will disable the function.

Parameters:

None.

Default Settings:

By default, Ping-detection of conflict is disabled.

Command Mode:

Global Configuration Mode.

Usage Guide:

To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.

Examples:

Enable Ping-detection of conflict.

```
Switch(config)#ip dhcp conflict ping-detection enable
```

Related Command:

ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

24.1.17 ip dhcp ping packets

Command:

ip dhcp ping packets <*request-num*>

no ip dhcp ping packets

Function:

Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.

Parameters:

<request-num> is the number of Ping request message to be sent in Ping-detection of conflict.

Default Settings:

No more than 2 Ping request messages will be sent by default.

Command Mode:

Global Configuration Mode.

Examples:

Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3.

```
Switch(config)#ip dhcp ping packets 3
```

Related Command:

ip dhcp conflict ping-detection enable, ip dhcp ping timeout

24.1.18 ip dhcp ping timeout

Command:

ip dhcp ping timeout <*timeout-value*>

no ip dhcp ping timeout

Function:

Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.

Parameters:

<timeout-value> is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.

Default Settings:

The timeout period is 500ms by default.

Command Mode:

Global Configuration Mode.

Examples:

Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms.

```
Switch(config)#ip dhcp conflict timeout 600
```

Related Command:

ip dhcp conflict ping-detection enable, ip dhcp ping packets

24.1.19 lease

Command:

lease { [<*days*>] [<*hours*>][<*minutes*>] | infinite }

no lease

Function:

Sets the lease time for addresses in the address pool; the "**no lease**" command restores the default setting.

Parameters:

<days> is number of days from 0 to 365;

<hours> is number of hours from 0 to 23;

<minutes> is number of minutes from 0 to 59;

infinite means perpetual use.

Default:

The default lease duration is 1 day.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.

Example:

Setting the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

```
Switch(dhcp-1-config)#lease 3 12 30
```

24.1.20 netbios-name-server

Command:

netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

Function:

Configures WINS servers' address; the "**no netbios-name-server**" command deletes the WINS server.

Parameters:

<address1>…<address8> are IP addresses, in decimal format.

Default:

No WINS server is configured by default.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.

Example:

Setting the server address of DHCP pool "1" to 192.168.1.1.

```
Switch(dhcp-1-config)#netbios-name-server 192.168.1.1
```

24.1.21 netbios-node-type

Command:

netbios-node-type {b-node | h-node | m-node | p-node | <*type-number*>}

no netbios-node-type

Function:

Sets the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameters:

b-node stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication;

m-node for hybrid node to communicate in point-to-point after broadcast; **p-node** for point-to-point node;

<type-number> is the node type in Hex from 0 to FF.

Default:

No client node type is specified by default.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example:

Setting the node type for client of pool 1 to broadcasting node.

```
Switch(dhcp-1-config)#netbios-node-type b-node
```

24.1.22 network-address

Command:

network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

Function:

Sets the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameters:

<network-number> is the network number;

<mask> is the subnet mask in the decimal format;

<prefix-length> stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default:

If no mask is specified, default mask will be assigned according to the address class.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command "hardware address" and "host".

Example:

Configuring the assignable address in pool 1 to be 10.1.128.0/24.

```
Switch(dhcp-1-config)#network-address 10.1.128.0 24
```

24.1.23 next-server

Command:

next-server <address1>[<address2>[…<address8>]]

no next-server

Function:

Sets the server address for storing the client import file; the "**no next-server**" command cancels the setting.

Parameters:

<address1>…<address8> are IP addresses, in the decimal format.

Command Mode:

DHCP Address Pool Mode

Usage Guide:

This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with "bootfile".

Example:

Setting the hosting server address as 10.1.128.4.

```
Switch(dhcp-1-config)#next-server 10.1.128.4
```

24.1.24 option

Command:

option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function:

Sets the network parameter specified by the option code; the "**no option <*code*>**"command cancels the setting for option.

Parameters:

<code> is the code for network parameters;

<string> is the ASCII string up to 255 characters;

<hex> is a value in Hex that is no greater than 510 and must be of even length;

<ipaddress> is the IP address in decimal format, up to 63 IP addresses can be configured.

Command Mode:

DHCP Address Pool Mode

Default:

None

Usage Guide:

The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example:

Setting the WWW server address as 10.1.128.240.

```
Switch(dhcp-1-config)#option 72 ip 10.1.128.240
```

24.1.25 service dhcp

Command:

service dhcp

no service dhcp

Function:

Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.

Parameters:

None

Default:

DHCP service is disabled by default.

Command mode:

Global Mode

Usage Guide:

Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example:

Enabling DHCP server.

```
Switch(config)#service dhcp
```

24.1.26 show ip dhcp binding

Command:

show ip dhcp binding [[<*ip-addr*>] [type {all | manual | dynamic}] [count]]

Function:

Displays IP-MAC binding information.

Parameters:

<ip-addr> is a specified IP address in decimal format;

all stands for all binding types (manual binding and dynamic assignment);

manual for manual binding;

dynamic for dynamic assignment;

count displays statistics for DHCP address binding entries.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch# show ip dhcp binding
IP address          Hardware address        Lease expiration      Type
10.1.1.233          00-00-E2-3A-26-04         Infinite          Manual
10.1.1.254          00-00-E2-3A-5C-D3          60               Automatic
```

Displayed information Explanation
IP address IP address assigned to a DHCP client
Hardware address MAC address of a DHCP client
Lease expiration Valid time for the DHCP client to hold the IP address
Type Type of assignment: manual binding or dynamic assignment.

24.1.27 show ip dhcp conflict

Command:

show ip dhcp conflict

Function:

Displays log information for addresses that have a conflict record.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch# show ip dhcp conflict
IP Address              Detection method      Detection Time
10.1.1.1                Ping                  FRI JAN 02 00:07:01 2002
```

Displayed information Explanation
IP Address Conflicting IP address
Detection method Method in which the conflict is detected.
Detection Time Time when the conflict is detected.

24.1.28 show ip dhcp server statistics

Command:

show ip dhcp server statistics

Function:

Displays statistics of all DHCP packets for a DHCP server.

Command mode:

Admin and Configuration Mode.

Example:

```
Switch# show ip dhcp server statistics
Address pools                   3
Database agents                 0
Automatic bindings              2
Manual bindings                 0
Conflict bindings               0
Expired bindings                0
Malformed message               0
```

```
Message                 Received
BOOTREQUEST             3814
DHCPDISCOVER            1899
DHCPREQUEST             6
DHCPDECLINE             0
DHCPRELEASE             1
DHCPINFORM              1

Message                 Send
BOOTREPLY               1911
DHCPOFFER               6
DHCPACK                 6
DHCPNAK                 0
DHCPRELAY               1907
DHCPFORWARD             0
Switch#
```

Displayed information Explanation
Address pools Number of DHCP address pools configured.
Database agents Number of database agents.
Automatic bindings Number of addresses assigned automatically
Manual bindings Number of addresses bound manually
Conflict bindings Number of conflicting addresses
Expired bindings Number of addresses whose leases are expired
Malformed message Number of error messages.
Message Received

Statistics for DHCP packets received
BOOTREQUEST Total packets received
DHCPDISCOVER Number of DHCPDISCOVER packets
DHCPREQUEST Number of DHCPREQUEST packets
DHCPDECLINE Number of DHCPDECLINE packets
DHCPRELEASE Number of DHCPRELEASE packets
DHCPINFORM Number of DHCPINFORM packets
Message Send Statistics for DHCP packets sent
BOOTREPLY Total packets sent
DHCPOFFER Number of DHCPOFFER packets
DHCPACK Number of DHCPACK packets
DHCPNAK Number of DHCPNAK packets
DHCPRELAY Number of DHCPRELAY packets
DHCPFORWARD Number of DHCPFORWARD packets

24.2 Commands for DHCP Relay Configuration

24.2.1 ip forward-protocol udp bootps

Command:

ip forward-protocol udp bootps

no ip forward-protocol udp bootps

Function:

Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp bootps**"command cancels the service.

Parameter:

bootps forwarding UDP port as 67 DHCP broadcast packets.

Default:

Not forward UPD broadcast packets by default.

Command mode:

Global Mode

Usage Guide:

The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example:

Setting DHCP packets to be forwarded to 192.168.1.5.

Switch(config)#ip forward-protocol udp boots
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5

24.2.2 ip helper-address

Command:

ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

Function:

Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address <*ip-address*>**" command cancels the setting.

Default:

None.

Command mode:

Interface Configuration Mode

Usage Guide:

The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after "**ip forward-protocol udp <*port*>**" command, the forwarding address configured by this command receives the UDP packets from **<*port*>**. The combination of "**ip forward-protocol udp <*port*>**" command and this command should be used for configuration.

Chapter 25 Commands for DHCPv6

25.1 clear ipv6 dhcp binding

Command:

clear ipv6 dhcp binding [*<ipv6-address>*] [pd*<ipv6-prefix* | *prefix-length>*]

Function:

To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records.

Parameter:

<ipv6-address> is the specified IPv6 address with binding record;

<ipv6-prefix*| *prefix-length> is the specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.

Command Mode:

Admin Configuration Mode.

Usage Guide:

DHCPv6 IPv6 address binding information can be displayed through the command show ipv6 dhcp binding. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.

Example:

To delete all binding record of IPv6 address and prefix.

```
Switch#clear ip dhcp binding
```

Relative Command:

show ipv6 dhcp binding

25.2 clear ipv6 dhcp server statistics

Command:

clear ipv6 dhcp server statistics

Function:

To delete the statistics of DHCPv6 Server, and reset DHCPv6 server counter.

Parameter:

None.

Command Mode:

Admin Mode.

Usage Guide:

Statistics about the DHCPv6 server can be displayed though the command **show ipv6 dhcp server statistics**, and these statistics can be reset with this command.

Example:

To reset DHCPv6 Server counter.

```
Switch#clear ip dhcp server statistics
```

Relative Command:

show ip dhcp server statistics

25.3 debug ipv6 dhcp client packet

Command:

debug ipv6 dhcp client {event | packet}

no debug ipv6 dhcp client {event | packet}

Function:

To enable the debugging messages for protocol packets of DHCPv6 prefix delegation client, the no form of this command will disable the debugging information.

Default:

Disabled.

Command Mode:

Admin Mode.

Example:

```
Switch# debug ipv6 dhcp client packet
```

25.4 debug ipv6 dhcp detail

Command:

debug ipv6 dhcp detail

no debug ipv6 dhcp detail

Function:

To display the debug information of all kinds of packets received or sent by DHCPv6, the no form of this command disabled this function.

Default:

Disabled.

Command Mode:

Admin Mode.

Example:

```
Switch# debug ipv6 dhcp detail
```

25.5 debug ipv6 dhcp relay packet

Command:

debug ipv6 dhcp relay packet

no debug ipv6 dhcp relay packet

Function:

To enable the debugging information for protocol packets of DHCPv6 relay, the no form of this command will disable the debugging.

Default:

Disabled.

Command Mode:

Admin Mode.

Example:

```
Switch# debug ipv6 dhcp relay packet
```

25.6 debug ipv6 dhcp server

Command:

debug ipv6 dhcp server { event | packet }

no debug ipv6 dhcp server { event | packet }

Function:

To enable the debugging information of DHCPv6 server, the no form of this command will disable the debugging.

Parameter:

event is to enable debugging messages for DHCPv6 server events, such as address allocation; packet is for debugging messages of protocol packets of DHCPv6 server.

Default:

Disabled.

Command Mode:

Admin Mode.

Example:

```
Switch#debug ipv6 dhcp server packet
```

25.7 dns-server

Command:

dns-server <*ipv6-address*>

no dns-server <*ipv6-address*>

Function:

To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration.

Parameter:

<ipv6-address> is the IPv6 address of DNS Server.

Default:

No configured address pool of DNS Server by default.

Command Mode:

DHCPv6 Address Pool Configuration Mode.

Usage Guide:

For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.

Example:

To configure the DNS Server address of DHCPv6 client as 2001:da8::1.

```
Switch(dhcp-1-config)#dns-server 2001:da8::1
```

25.8 domain-name

Command:

domain-name <*domain-name*>

no domain-name <*domain-name*>

Function:

To configure domain name of DHCPv6 client; the no form of this command will delete the domain name.

Parameter:

<domain-name> is the domain name, less than 32 characters.

Command Mode:

DHCPv6 Address Pool Configuration Mode.

Default:

The domain name parameter of address pool is not configured by default.

Usage Guide:

At most 3 domain names can be configured for each address pool.

Example:

To set the domain name of DHCPv6 client as test.com.cn

```
Switch(dhcp-1-config)#domain-name test.com.cn
```

25.9 excluded-address

Command:

excluded-address <*ipv6-address*>

no excluded-address <*ipv6-address*>

Function:

To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration.

Parameter:

<ipv6-address> is the IPv6 address to be excluded from being allocated to hosts in the address pool.

Default:

Disabled

Command Mode:

DHCPv6 address pool configuration mode.

Usage Guide:

This command is used to preserve the specified address from DHCPv6 address allocation.

Example:

To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation.

```
Switch(config)#excluded-address 2001:da8:123::1
```

25.10 ipv6 address

Command:

ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

Function:

To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation.

Parameters:

<prefix-name> is a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool. ***<ipv6-prefix/prefix-length>*** is latter part of the IPv6 address excluding the address prefix, as well as its length.

Command Mode:

Interface Configuration Mode.

Default:

No global address is configured for interfaces by default.

Usage Guide:

The IPv6 address of an interface falls into two parts: ***<prefix-name>*** and ***<ipv6-prefix>/<prefix-length>***. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by ***<prefix-name>*** and ***<ipv6-prefix/prefix-length>*** combination will be removed, and the advertising of the prefix will be disabled. Only one ***<ipv6-prefix/prefix-length>*** can be configured for one prefix name.

Example:

If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1.

```
Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64
```

25.11 ipv6 dhcp client pd

Command:

ipv6 dhcp client pd *<prefix-name>* [rapid-commit]

no ipv6 dhcp client pd

Function:

To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix.

Parameters:

<prefix-name> is the string with its length no more than 32, which designates the name of the address prefix. If **rapid-commit** optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.

Command Mode:

Interface Configuration Mode.

Default:

DHCPv6 prefix delegation client is not enabled by default.

Usage Guide:

This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.

Example:

```
Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit
```

25.12 ipv6 dhcp client pd hint

Command:

ipv6 dhcp client pd hint *<prefix|prefix-length>*

no ipv6 dhcp client pd hint *<prefix|prefix-length>*

Function:

Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface.

Parameters:

<prefix|prefix-length> means the prefix demanded by the client and its length.

Command Mode:

Interface Configure Mode.

Default Settings:

There is no such configuration in the system by default.

Usage Guide:

The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.

Examples:

```
Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48
```

25.13 ipv6 dhcp pool

Command:

ipv6 dhcp pool <*poolname*>

no ipv6 dhcp pool <*poolname*>

Function:

To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool.

Parameter:

< *poolname*> is the address pool name of DHCPv6 with its length no more than 32.

Default:

Any DHCPv6 address pool are not configured by default.

Command Mode:

Global Mode.

Usage Guide:

This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example:

To define an address pool, named 1.

```
Switch(config)#ipv6 dhcp pool 1
```

25.14 ipv6 dhcp relay destination

Command:

ipv6 dhcp relay destination {[<ipv6-address>] [interface { <interface-name> | vlan <1-4096> }] }

no ipv6 dhcp relay destination { [<ipv6-address>] [interface { <interface-name> | vlan <1-4096> }] }

Function:

To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration.

Parameters:

<ipv6-address> is the address of the destination to which the DHCPv6 relay forwards; ***<interface-name>*** or VLAN is the interface name or VLAN id which is used for forwarding of DHCPv6 requests, ***<interface-name>*** should be a lay three VLAN name, and the VLAN id is limited between 1 and 4096. If **<ipv6-addess>** is a global unicast address, the **interface** parameter should not be configured; If **<ipv6-address>** is an local address, the **interface** parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of **ALL_DHCP_Servers (FF05::1:3),** if the interface parameter is configured only.

Command Mode:

Interface Configuration Mode.

Default:

By default, destination address for DHCPv6 relay is not configured.

Usage Guide:

This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to

25.15 ipv6 dhcp server

Command:

ipv6 dhcp server <*poolname*> [preference <*value*>] [rapid-commit] [allow-hint]

no ipv6 dhcp server

Function:

This command configures the address pool which will be allocated by the DHCPv6 server through t he specified interface. The no form of this command will remove the address pool configuration.

Parameters:

<poolname> is a string with its length less than 32, which designates the name of the address pool which is associated with the specified interface. If the **rapid-commit** option has been specified, the DHCPv6 server send a REPLY packet to the client immediately after receiving the SOLICIT packet. If the **preference** option has been specified, ***<value>*** will be the priority of the DHCPv6 server, with its value allowed between 0 and 255, and with 0 by default, the bigger the preference value is, the higher the priority of the DHCPv6 server. If the **allow-hint** option has been specified, the client expected value of parameters will be appended in its request packets.

Command Mode:

Interface Configuration Mode.

Default:

DHCPv6 address pool based on port is not configured by default.

Usage Guide:

This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One port only can configure the one DHCPv6 address pool.

Example:

```
Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint
```

25.16 ipv6 general-prefix

Command:

ipv6 general-prefix <*prefix-name*> <*ipv6-prefix/prefix-length*>

no ipv6 general-prefix <*prefix-name*>

Function:

To define an IPv6 general prefix. The no form of this command will delete the configuration.

Parameter:

<prefix-name> is a character string less than 32 characters, to use as IPv6 general prefix name. ***<ipv6-prefix/prefix-length>*** is defined as IPv6 general prefix.

Command Mode:

Global Mode.

Default:

IPv6 general prefix is not configured by default.

Usage Guide:

If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix can not use the same prefix definition with prefixes learnt from prefix delegation.

Example:

To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.

```
Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48
```

25.17 ipv6 local pool

Command:

ipv6 local pool *<poolname> <prefix/prefix-length> <assigned-length>*

no ipv6 local pool *<poolname>*

Function:

To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration.

Parameters:

<poolname> is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32.

<prefix/prefix-length> is the address prefix and its length of the prefix delegation. ***<assigned-length>*** is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of ***<prefix-length>***

Command Mode:

Global Mode.

Default:

No IPv6 prefix delegation address pool is configured by default.

Usage Guide:

This command should be used with the "**prefix delegation pool**" command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated "**prefix delegation**" command will be in-effective either.

25.18 lifetime

Command:

lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity}

no lifetime

Function:

To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.

Parameters:

<valid-time> **and** ***<preferred-time>*** are the valid life time and preferred life time respectively for the allocated IPv6 addresses in the local address pool. Its value is allowed to be between 1 and 31536000 in seconds, and ***<preferred-time>*** should never be bigger than ***<valid-time>***. The **infinity** parameter designates the maximum life time.

Command Mode:

DHCPv6 Address Pool Configuration Mode.

Default:

The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively.

Example:

To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds.

```
Switch(config)#lifetime 1000 600
```

25.19 network-address

Command:

network-address ***<ipv6-pool-start-address>*** **{<*ipv6-pool-end-address*> | <*prefix-length*>} [eui-64]**

no network-address

Function:

To configure the DHCPv6 address pool; the no form of this command will remove the address pool configuration.

Parameters:

<ipv6-pool-start-adderss> is the start of the address pool;

<ipv6-pool-end-address> is the end of the address pool;

<prefix-length> is the length of the address prefix, which is allowed to be between 3 and 128, and 64 by default, the size of the pool will be determined by ***<prefix-length>*** if it has been specified. ***<ipv6-pool-end-address>*** and ***<prefix-length>*** alternative options to determine the size of the IPv6 address pool. If ***<prefix-length>*** is 64 and the **eui-64** option has been configured, the DHCPv6 server will allocate IPv6 addresses according to the EUI-64 standard, or the DHCPv6 server will be allocating addresses sequentially.

Default:

No address pool is configured by default.

Command Mode:

DHCPv6 Address Pool Configuration Mode.

Usage Guide:

This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If ***<ipv6-pool-end-address>*** is bigger than ***<ipv6-pool-start-address>***, this command returns at once.

Example:

To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200.

```
Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200
```

Relative Command:

excluded-address

25.20 prefix-delegation

Command:

prefix-delegation *<ipv6-prefix/prefix-length>* <client-DUID> [iaid <iaid>] [lifetime { <valid-time> | infinity} { *<preferred-time>* | infinity}]

no prefix-delegation <ipv6-prefix/prefix-length> *<client-DUID>* [iaid *<iaid>*]

Function:

To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation.

Parameters:

<ipv6-prefix/prefix-length> is the length of the prefix to be allocated to the client. ***<client-DUID>*** is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters. ***<iaid>*** is the value to be appended in the IA_PD field of the clients' requests. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, <preferred-time> should never be bigger than <valid-time>. If not configured, the default <valid-time> will be 2592000, while <preferred-time> will be 604800. The infinity parameter means the life time is infinity.

Command Mode:

DHCPv6 Address Pool Configuration Mode.

Default:

Disabled.

Usage Guide:

This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.

Example:

The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12.

```
Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 00010006000000005000BBFAA2408 iaid 12
```

25.21 prefix-delegation pool

Command:

prefix-delegation pool <*poolname*> [lifetime { <*valid-time*> | infinity} { <*preferred-time*> | infinity}]

no prefix-delegation pool <*poolname*>

Function:

To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration.

Parameters:

<poolname> is the name of the address prefix pool, the length name string should be less than 32. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, <preferred-time> should never be bigger than <valid-time>. If not configured, the default <valid-time> will be 2592000, while <preferred-time> will be 604800. The infinity parameter means the life time is infinity.

Command Mode:

DHCPv6 address pool configuration mode.

Default:

The prefix delegation name used by DHCPv6 address pool is not configured.

Usage Guide:

This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.

Example:

```
Switch(dhcp-1-config)#prefix-delegation pool abc
```

25.22 service dhcpv6

Command:

service dhcpv6

no service dhcpv6

Function:

To enable DHCPv6 server function; the no form of this command disables the configuration.

Parameter:

None.

Default:

Disabled.

Command Mode: G

lobal Mode.

Usage Guide:

The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.

Examp:

To enable DHCPv6 server.

```
Switch(config)#service dhcpv6
```

25.23 show ipv6 dhcp

Command:

show ipv6 dhcp

Function:

To show the enable switch and DUID of DHCPv6 service.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To show the enable switch and DUID of DHCPv6 service, this command only can support the DUID type of DUID-LLT. The DUID types are the same not only displayed but also required in client and server identifier options.

Example:

```
Switch#show ipv6 dhcp
DHCPv6 is enabled
DUID is <000100060000000500030f112233>
```

25.24 show ipv6 dhcp binding

Command:

show ipv6 dhcp binding [*<ipv6-address>*| pd *<ipv6-prefix*|*prefix-length>*|count]

Function:

To show all the address and prefix binding information of DHCPv6.

Parameter:

<ipv6-address> is the specified IPv6 address; **count** show the number of DHCPv6 address bindings.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.

Example:

```
Switch#show ipv6 dhcp binding
Client: iatype IANA, iaid 0x0e001d92
DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
IANA leased address: 2001:da8::10
Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
Lease obtained at %Jan 01 01:34:44 1970
Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1
```

25.25 show ipv6 dhcp interface

Command:

show ipv6 dhcp interface [<*interface-name*>]

Function:

To show the information for DHCPv6 interface.

Parameter:

<interface-name> is the name and number of interface, if the***<interface-name>*** parameter is not provided, then all the DHCPv6 interface information will be shown.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client、DHCPv6 server、DHCPv6 relay) , and the relative conformation information under all kinds of mode.

Example:

```
Switch#show ipv6 dhcp interface vlan10
Vlan10 is in server mode
Using pool: poolv6
Preference value: 20
Rapid-Commit is disabled
```

25.26 show ipv6 dhcp local pool

Command:

show ipv6 dhcp local pool

Function:

To show the statistic information of DHCPv6 prefix pool.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.

Example:

```
Switch#show ipv6 dhcp pool binding
```

25.27 show ipv6 dhcp pool

Command:

show ipv6 dhcp pool [<*poolname*>]

Function:

To show the DHCPv6 address pool information.

Parameter:

<poolname> is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the ***<poolname>*** parameter is not provided, then all the DHCPv6 address pool information will be shown. ,

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server.

Example:

```
Switch#show ipv6 dhcp pool poolv6
```

25.28 show ipv6 dhcp statistics

Command:

show ipv6 dhcp statistics

Function:

To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Command Mode:

Admin and Configuration Mode.

Example:

```
Switch#show ipv6 dhcp server statistics
Address pools                    1
Active bindings                  0
Expiried bindings                0
Malformed message                0

Message                    Recieved
DHCP6SOLICIT                  0
DHCP6ADVERTISE                0
DHCP6REQUEST                  0
```

```
DHCP6REPLY                0
DHCP6RENEW                0
DHCP6REBIND               0
DHCP6RELEASE              0
DHCP6DECLINE              0
DHCP6CONFIRM              0
DHCP6RECONFIGURE          0
DHCP6INFORMREQ            0
DHCP6RELAYFORW            0
DHCP6RELAYREPLY           0

Message                   Send
DHCP6SOLICIT              0
DHCP6ADVERTISE            0
DHCP6REQUEST              0
DHCP6REPLY                0
DHCP6RENEW                0
DHCP6REBIND               0
DHCP6RELEASE              0
DHCP6DECLINE              0
DHCP6CONFIRM              0
DHCP6RECONFIGURE          0
DHCP6INFORMREQ            0
DHCP6RELAYFORW            0
DHCP6RELAYREPLY           0
```

Show information Explanation
Address pools To configure the number of DHCPv6 address pools;
Active bindings The number of auto assign addresses;
Expiried bindings The number of expiried bindings;
Malformed message The number of malformed messages;
Message Recieved The statistic of received DHCPv6 packets.

DHCP6SOLICIT The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST The number of DHCPv6 REQUEST packets.
DHCP6REPLY The number of DHCPv6 REPLY packets.
DHCP6RENEW The number of DHCPv6 RENEW packets.
DHCP6REBIND The number of DHCPv6 REBIND packets.
DHCP6RELEASE The number of DHCPv6 RELEASE packets.
DHCP6DECLINE The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY The number of DHCPv6 RELAYREPLY packets.
Message Send The statistic of sending DHCPv6 packets
DHCP6SOLICIT

The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST The number of DHCPv6 REQUEST packets.
DHCP6REPLY The number of DHCPv6 REPLY packets.
DHCP6RENEW The number of DHCPv6 RENEW packets.
DHCP6REBIND The number of DHCPv6 REBIND packets.
DHCP6RELEASE The number of DHCPv6 RELEASE packets.
DHCP6DECLINE The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW The number of DHCPv6 RELAYFORW packets.

25.29 show ipv6 general-prefix

Command:

show ipv6 general-prefix

Function:

To show the IPv6 general prefix pool information.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example:

```
Switch#show ipv6 general-prefix
```

Chapter 26 Commands for DHCP Option 82

26.1 ip dhcp relay information option

Command:

ip dhcp relay information option

no ip dhcp relay information option

Function:

Set this command to enable the option82 function of the switch Relay Agent. The "**no ip dhcp relay information option**" command is used to disable the option82 function of the switch Relay Agent.

Parameters:

None.

Default Settings:

The system disables the option82 function by default.

Command Mode:

Global configuration mode

Usage Guide:

Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.

Example:

Enable the option82 function of the Relay Agent.

Switch(config)#service dhcp
Switch(config)# ip forward-protocol udp bootps
Switch(config)# ip dhcp relay information option

26.2 ip dhcp relay information policy

Command:

ip dhcp relay information policy {drop | keep | replace

no ip dhcp relay information policy

Function:

This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The "no ip dhcp relay information policy" will set the retransmitting policy of the option 82 DCHP message as "replace".

Parameters:

None

Command Mode:

Interface configuration mode.

Default Settings:

The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.

User Guide:

Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.

Example:

Set the retransmitting policy of DHCP messages option 82 as keep.

```
Switch(Config-if-Vlan1)# ip dhcp relay information policy keep
```

26.3 ip dhcp relay information option subscriber-id

Command:

ip dhcp relay information option subscriber-id {standard | <*circuit-id*>}

no ip dhcp relay information option subscriber-id

Function:

This command is used to set the format of option82 sub-option1(Circuit ID option) added to the DHCP request messages from interface, **standard** means the standard vlan name and physical port name format, like"Vlan2+Ethernet0/0/12",***<circuit-id>*** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters. The" **no ip dhcp relay information option subscriber-id**" command will set the format of added option82 sub-option1 (Circuit ID option) as standard format.

Parameters:

None

Command Mode:

Interface configuration mode.

Default Settings:

The system uses the standard format to set the circuit-id of option 82 by default.

User Guide:

Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.

Example:

Set the sub-option circuit-id of DHCP option82 as foobar.

```
Switch(config)# ip dhcp relay information option subscriber-id foobar
```

26.4 ip dhcp server relay information enable

Command:

ip dhcp server relay information enable

no ip dhcp server relay information enable

Function:

This command is used to enable the switch DHCP server to identify option82. The “no ip dhcp server relay information enable” command will make the server ignore the option 82.

Parameters:

None

Command Mode:

Global configuration mode

Default Setting:

The system disable the option82 identifying function by default.

User Guide:

If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.

Example:

Set the DHCP server to support option82

```
Switch(Config-if-Vlan1)# ip dhcp server relay information enable
```

26.5 show ip dhcp relay information option

Command:

show ip dhcp relay information option

Function:

This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.

Parameters:

None.

Command Mode:

Admin and Configuration Mode.

User Guide:

Use this command to check the state information of Relay Agent option82 during operation.

Example:

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is disabled
ip dhcp relay information option(i.e. option 82) is enabled
Vlan2:
        ip dhcp relay information policy keep
        ip dhcp relay information option subscriber-id standard
```

```
Vlan3:
        ip dhcp relay information policy replace
        ip dhcp relay information option subscriber-id foobar
```

26.6 debug ip dhcp relay packet

Command:

debug ip dhcp relay packet

Function:

This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.

Parameters:

None

Command Mode:

Admin Mode.

User Guide:

Use this command during the operation to display the procedure of data packets processing of the server and to display the corresponding option82 operation information. Identified option 82 information of the request message and the option 82 information returned by the reply message.

Example:

Display the information of data packets processing in DHCP Relay Agent.

```
Switch(config)# debug ip dhcp relay packet
```

Chapter 27 Commands for DHCP Snooping

27.1 debug ip dhcp snooping packet interface

Command:

debug ip dhcp snooping packet interface {[ethernet] *<InterfaceName>*}

no debug ip dhcp snooping packet {[ethernet] *<InterfaceName>*}

Function:

This command is used to enable the DHCP SNOOPING debug switch to debug the information that DHCP SNOOPING is receiving a packet.

Parameters:

<InterfaceName>: Interface name.

Command Mode:

Admin Mode.

Usage Guide:

The information that DHCP Snooping is receiving messages from a specific port.

27.2 debug ip dhcp snooping packet

Command:

debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Function:

This command is used to enable the DHCP SNOOPING debug switch to debug the message-processing procedure of DHCP SNOOPING.

Command Mode:

Admin Mode.

Usage Guide:

The debug information that the DHCP SNOOPING is processing messages, including every step in the message-processing procedure: adding alarm information, adding binding information, transmitting DHCP messages, adding/peeling option 82 and etc.

27.3 debug ip dhcp snooping update

Command:

debug ip dhcp snooping update

no debug ip dhcp snooping update

Function:

This command is use to enable the DHCP snooping debug switch to debug the communication information between DHCP snooping and helper server.

Command Mode:

Admin Mode.

Usage Guide:

Debug the information of communication messages received and sent by DHCP snooping and helper server.

27.4 debug ip dhcp snooping event

Command:

debug ip dhcp snooping event

no debug ip dhcp snooping event

Function:

This command is use to enable the DHCP SNOOPING debug switch to debug the state of DHCP SNOOPING task.

Command Mode:

Admin mode.

Usage Guide:

This command is mainly used to debug the state of DHCP SNOOPING task and available of outputting the state of checking binding data and executing port action and so on.

27.5 debug ip dhcp snooping binding

Command:

debug ip dhcp snooping binding

no debug ip dhcp snooping binding

Function:

This command is use to enable the DHCP SNOOPING debug switch to debug the state of binding data of DHCP SNOOPING.

Command Mode:

Admin mode

Usage Guide:

This command is mainly used to debug the state of DHCP SNOOPING task when it adds ARP list entries, dot1x users and trusted user list entries according to binding data.

27.6 ip dhcp snooping

Command:

ip dhcp snooping enable

no ip dhcp snooping enable

Function:

Enable the DHCP Snooping function.

Parameters:

None.

Command Mode:

Globe mode.

Default Settings:

DHCP Snooping is disabled by default.

Usage Guide:

When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.

Example:

Enable the DHCP Snooping function.

```
switch(config)#ip dhcp snooping enable
```

27.7 ip dhcp snooping binding

Command:

ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function:

Enable the DHCP Snooping binding funciton

Parameters:

None.

Command Mode:

Globe mode

Default Settings:

DHCP Snooping binding is disabled by default.

Usage Guide:

When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.

Example:

Enable the DHCP Snooping binding funciton.

```
switch(config)#ip dhcp snooping binding enable
```

Relative Command:

ip dhcp snooping enable

27.8 ip dhcp snooping binding user

Command:

ip dhcp snooping binding user <*mac*> address <*ipaddress*> <*mask*> vlan <*vid*> interface [Ethernet] <*ifname*>

no ip dhcp snooping binding user <*mac*> interface [Ethernet] <*ifname*>

Function:

Configure the information of static binding users

Parameters:

<*mac*>: The MAC address of the static binding user, whic is the only index of the binding user.

<*ipaddress*> <*mask*>: The IP address and mask of the static binding user.

<*vid*>: The VLAN ID which the static binding user belongs to.

<*ifname*>: The access interface of static binding user.

Command Mode:

Globe mode

Default Settings:

DHCP Snooping has no static binding list entry by default.

Usage Guide:

The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.

Example:

Configure static binding users.

```
switch(config)#ip dhcp snooping binding user 00-30-4f-12-34-56 address 192.168.1.16 255.255.255.0 interface Ethernet 1/16
```

Relative Command:

ip dhcp snooping binding enable

27.9 ip dhcp snooping binding arp

Command:

ip dhcp snooping binding arp

no ip dhcp snooping binding arp

Function:

Enable the DHCP Snooping binding ARP funciton.

Parameters:

None

Command Mode:

Globe mode

Default Settings:

DHCP Snooping binding ARP funciton is disabled by default.

Usage Guide:

When this function is enbaled, DHCP SNOOPING will add binding ARP list entries according to binding information. Only after the binding function is enabled, can the binding ARP function be enabled. Binding ARP list entries are static entries without configuration of reservation, and will be added to the NEIGHBOUR list directly. The priority of binding ARP list entries is lower than the static ARP list entries set by administrator, so can be overwritten by static ARP list entries; but, when static ARP list entries are deleted, the binding ARP list entries can not be recovered untill the DHCP SNOOPING recapture the biding inforamtion. Adding binding ARP list entries is used to prevent these list entried from being attacked by ARP cheating. At the same time, these static list entries need no reauthenticaiton, which can prenvent the switch from the failing to reauthenticate ARP when it is being attacked by ARP scanning.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example:

Enable the DHCP Snooping binding ARP funciton.

```
switch(config)#ip dhcp snooping binding arp
```

Relative Command:

ip dhcp snooping binding enable

27.10 ip dhcp snooping binding dot1x

Command:

ip dhcp snooping binding dot1x

no ip dhcp snooping binding dot1x

Function:

Enable the DHCP Snooping binding DOT1X funciton.

Parameters:

None

Command Mode:

Port mode

Default Settings:

By default, the binding DOT1X funciton is disabled on all ports.

Usage Guide:

When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to"ip dhcp snooping binding user-contro"command.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example:

Enable the binding DOT1X funciton on port ethernet1/1.

switch(config)#interface ethernet 1/1
switch(Config- Ethernet 1/1)# ip dhcp snooping binding dot1x

Relative Command:

ip dhcp snooping binding enable

ip dhcp snooping binding user-control

27.11 ip dhcp snooping binding user-control

Command:

ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Function:

Enable the binding user funtion.

Parameters:

None.

Command Mode:

Port Mode.

Default Settings:

By default, the binding user funciton is disabled on all ports.

Usage Guide:

When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to" ip dhcp

snooping binding dot1x“ command.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example:

Enable the binding USER funciton on port ethernet1/1.

```
switch(config)#interface ethernet 1/1
switch(Config- Ethernet 1/1)# ip dhcp snooping binding user-control
```

Relative Command:

ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

27.12 ip dhcp snooping binding user-control max-user

Command:

ip dhcp snooping binding user-control max-user *<number>*

no ip dhcp snooping binding user-control max-user

Function:

Set the max number of users allowed to access the port when enabling DHCP Snooping binding user funciton; the no operation of this command will restore default value.

Parameters:

<number> the max number of users allowed to access the port, from 0 to 1024.

Command Mode:

Port Configuration Mode.

Default Settings:

The max number of users allowed by each port to access is 1024.

Usage Guide:

This command defines the max number of trust users distributed according to binding information, with **ip dhcp snooping binding user-contrl** enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding informaiton of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binging informaiton accordint to the new smaller max user number. When the number of distributed bingding informaiton entries reaches the max limit, no new DHCP will be able to become trust user or to access other network resouces via the switch.

Examples:

Enable DHCP Snooping binding user funtion on Port ethernet1/1, setting the max number of user allowed to access by Port Ethernet1/1 as 5.

```
Switch(Config-If-Ethernet1/1)# ip dhcp snooping binding user-control max-user 5
```

Related Command:

ip dhcp snooping binding user-control

27.13 ip dhcp snooping trust

Command:

ip dhcp snooping trust

no ip dhcp snooping trust

Function:

Set or delete the DHCP Snooping trust attributes of a port.

Parameters:

None

Command Mode:

Port mode

Default Settings:

By default, all ports are non-trusted ports

Usage Guide:

Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log).

Example:

Set port ethernet1/1 as a DHCP Snooping trusted port

switch(config)#interface ethernet 1/1
switch(Config- Ethernet 1/1)#ip dhcp snooping trust

27.14 ip dhcp snooping action

Command:

ip dhcp snooping action {shutdown | blackhole} [recovery <*second*>]

no ip dhcp snooping action

Function:

Set or delete the automatic defense action of a port.

Parameters:

shutdown: When the port detects a fake DHCP Server, it will be shutdown.

blackhole: When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.

recovery: Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole）.

second: Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.

Command Mode:

Port mode

Default Settings:

No default defense action.

Usage Guide:

Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not

detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.

Example:

Set the DHCP Snooping defense action of port ethernet1/1 as setting blackhole, and the recovery time is 30 seconds.

```
switch(config)#interface ethernet 1/1
switch(Config-Ethernet1/1)#ip dhcp snooping action blackhole recovery 30
```

27.15 ip dhcp snooping action MaxNum

Command:

ip dhcp snooping action {<maxNum>|default}

Function:

Set the number of defense action that can be simultaneously take effect.

Parameters:

<maxNum>: the number of defense action on each port, the range of which is 1-200, and the value f which is 10 by default.

default: recover to the default value.

Command Mode:

Globe mode

Default Settings:

The default value is 10.

Usage Guide:

Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.

Example:

Set the number of port defense actions as 100.

```
switch(config)#ip dhcp snooping action 100
```

27.16 ip dhcp snooping limit-rate

Command:

ip dhcp snooping limit-rate <*pps*>

no ip dhcp snooping limit-rate

Function:

Set the DHCP message rate limit

Parameters:

<pps>: The number of DHCP messages transmitted in every minute, ranging from 0 to 100. Its default value is 100. 0 means that no DHCP message will be transmitted.

Command Mode:

Globe mode

Default Settings:

The default value is 100.

Usage Guide:

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The software performance of the switch is relative to the type of the switch, its current load and so on. DCRS-5950 switch message rate limit is 100pps.

Example:

Set the message transmission rate as 50pps.

```
switch(config)#ip dhcp snooping limit-rate 50
```

27.17 ip dhcp snooping information enable

Command:

ip dhcp snooping information enable

no ip dhcp snooping information enable

Function:

This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function.

Parameters:

None.

Default Settings:

Option 82 function is disabled in DHCP Snooping by default.

Command Mode:

Global Configuration Mode.

Usage Guide:

Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like “vlan1+ethernet1/12”. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like “00030f023301”. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it. This command and “**ip dhcp snooping option82 enable**” command are mutually exclusive.

Examples:

Enable option 82 function of DHCP Snooping on the switch.

```
Switch(config)#ip dhcp snooping enable
```

```
Switch(config)# ip dhcp snooping binding enable
```

```
Switch(config)# ip dhcp snooping information enable
```

27.18 ip dhcp snooping option82 enable

Command:

ip dhcp snooping option82 enable

no ip dhcp snooping option82 enable

Function:

To enable DHCP option82 of dot1x in access switch. After DHCP Snooping monitored DHCP requires packets, add the option82 which can indicate user authentication state to the back of requires packet, and then deliver to DHCP relay.

Parameter:

None.

Command Mode:

Global Mode.

Default:

The DHCP option82 of dot1x is disabled by default.

Usage Guide:

This command configures the DHCP snooping to append the option82 information for DHCP requests when dot1x dhcpoption82based authentication is applied. By default, for un-authenticated users, the switch appends to the option 82 field of the DHCP requests with the remote-id field as unauth, and the circuit-id field as the MAC address of the CPU port of the switch. The DHCP server allocates addresses based on the information provided by the option82 field. And users can retrieve different IP addresses before and after authentication. When this command is applied, DHCP relay should not be configured on the truck switch which is connected to the local access switch.

Example:

Enable option82 function of DHCP Snooping.

```
switch(Config)#ip dhcp snooping option82 enable
```

Relative Command:

dot1x port-method dhcpoption82based

27.19 enable trustview key

Command:

enable trustview key {0 | 7} <*password*>

no enable trustview key

Function:

To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not.

Parameter:

<password> is character string length less than 16, which use as encrypted key. 0 for un-encrypted text for the password, while 7 for encrypted.

Command Mode:

Global Mode.

Default:

Disabled.

Usage Guide:

The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.

Example:

Enable encrypt or hash function of private message.

```
Switch(config)# enable trustview key 0 digitalchina
```

27.20 ip user helper-address

Command:

ip user helper-address <*svr_addr*> [port <*udp_port*>] source <*src_addr*> [secondary]

no ip user helper-address [secondary]

Function:

Set the address and port of HELPER SERVER.

Parameters:

<*svr_addr*>: The IP address of HELPER SERVER 的 IP in dotted-decimal notation.

udp_port: The UDP port of HELPER SERVER, the range of which is1－65535, and its default value is 9119.

src_addr: The local management IP address of the switch, in dotted-decimal notation.

sencondary: Whether it is a secondary SERVER address.

Command Mode:

Global mode

Default Settings:

There is no HELPER SERVER address by default.

Usage Guide:

DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into server packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of "**dot1x configuration**".

Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER.

Please pay attention:

source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.

Example:

Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value.

```
switch(config)#interface vlan 1
```

```
switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0
switch(Config-if-Vlan1)exit
switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1
```

27.21 show trustview status

Command:

show trustview status

Function:

To show all kinds of private packets state information, which sending or receiving from TrustView (inter security management background system) of PLANET.

Parameter:

None.

Command Mode:

Admin and Configuration Mode.

Default:

None.

Usage Guide:

This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example:

```
Switch#show trustview status
Primary TrustView Server 200.101.0.9:9119
    TrustView version2 message inform successed
    TrustView inform free resource successed
    TrustView inform web redirect address successed
    TrustView inform user binding data successed
TrustView version2 message encrypt/digest enabled
Key: 08:02:33:34:35:36:37:38
Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages
Sent 106 encrypted messages
Free resource is 200.101.0.9/255.255.255.255
Web redirect address for unauthencated users is <http://200.101.0.9:8080>
Rcvd 0 force log-off packets
Rcvd 19 force accounting update packets
Using version two private packet
```

27.22 show ip dhcp snooping

Command:

show ip dhcp snooping [interface [ethernet] <*interfaceName*>]

Function:

Display the current cofiguration information of dhcp snooping or display the records of defense actions of a specific port.

Parameters:

***<interfaceName>*:** The name of the specific port.

Command Mode:

Admin and Configuration Mode.

Default Settings:

None.

Usage Guide:

If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port.

Example:

```
switch#show ip dhcp snooping
DHCP Snooping is enabled

DHCP Snooping binding arp: disabled
DHCP Snooping maxnum of action info:10
DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456
DHCP Snooping droped packets: 0, discarded packets: 0
DHCP Snooping alarm count: 0, binding count: 0,
      expired binding: 0, request binding: 0

interface          trust        action       recovery     alarm num    bind num
---------------- --------- --------- ---------- --------- ----------
Ethernet1/1      trust       none         0second      0             0
Ethernet1/2      untrust     none         0second      0             0
Ethernet1/3      untrust     none         0second      0             0
Ethernet1/4      untrust     none         0second      0             1
Ethernet1/5      untrust     none         0second      2             0
Ethernet1/6      untrust     none         0second      0             0
Ethernet1/7      untrust     none         0second      0             0
Ethernet1/8      untrust     none         0second      0             1
Ethernet1/9      untrust     none         0second      0             0
Ethernet1/10     untrust     none         0second      0             0
Ethernet1/11     untrust     none         0second      0             0
Ethernet1/12     untrust     none         0second      0             0
Ethernet1/13     untrust     none         0second      0             0
Ethernet1/14     untrust     none         0second      0             0
Ethernet1/15     untrust     none         0second      0             0
Ethernet1/16     untrust     none         0second      0             0
```

Ethernet1/17	untrust	none	0second	0	0
Ethernet1/18	untrust	none	0second	0	0
Ethernet1/19	untrust	none	0second	0	0
Ethernet1/20	untrust	none	0second	0	0
Ethernet1/21	untrust	none	0second	0	0
Ethernet1/22	untrust	none	0second	0	0
Ethernet1/23	untrust	none	0second	0	0
Ethernet1/24	untrust	none	0second	0	0

Displayed Information Explanation
DHCP Snooping is enable Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info The number limitation of port defense actions
DHCP Snooping limit rate The rate limitation of receiving packets
switch ID The switch ID is used to identify the switch, usually using the CPU MAC address.
DHCP Snooping droped packets The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count: The number of alarm information.
binding count The number of binding information.

expired binding The number of binding information which is already expired but has not been deleted. The reason why the expired information is not deleted immediately might be that the switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding The number of REQUEST information
interface The name of port
trust The truest attributes of the port
action The automatic defense action of the port
recovery The automatic recovery time of the port
alarm num The number of history records of the port automatic defense actions
bind num The number of port-relative binding information.

```
switch#show ip dhcp snooping int Ethernet1/1
interface Ethernet1/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
Alarm info: 0

Binding info: 0

Expired Binding: 0

Request Binding: 0
```

Displayed Information Explanation
interface The name of port
trust attribute The truest attributes of the port
action The automatic defense action of the port
recovery interval The automatic recovery time of the port
maxnum of alarm info The max number of automatic defense actions that can be recorded by the port
binding dot1x Whether the binding dot1x function is enabled on the port
binding user Whether the binding user function is enabled on the port.
Alarm info The number of alarm information.
Binding info The number of binding information.
Expired Binding The expired binding information
Request Binding REQUEST information

Chapter 28 Commands for DHCPv6 Snooping

28.1 clear ipv6 dhcp snooping binding

Command:

clear ipv6 dhcp snooping binding {*<MAC>* | *<ipv6 address>* | interface {ethernet *<IFNAME>*|*<IFNAME>*} | all}

Function:

Clear DHCPv6 Snooping binding.

Parameter:

MAC: Delete the binding of the specific MAC address

ipv6 address: Delete the binding of the specific IPv6 address

IFNAME: The port name

all: Delete all binding of DHCPv6 Snooping

Command Mode:

Admin mode

Default:

None

Usage Guide:

Delete the (one port or all ports) dynamic DHCPv6 Snooping binding information.

Example:

Clear all dynamic binding of DHCPv6 Snooping.

```
switch#clear ipv6 dhcp snooping binding all
```

28.2 debug ipv6 dhcp snooping binding

Command: .

debug ipv6 dhcp snooping binding

Function:

Debug the binding information of DHCPv6 Snooping.

Parameter:

None

Command Mode:

Admin mode

Default:

None

Usage Guide:

Display the binding processing information of DHCPv6 Snooping, include: create/delete the binding.

Example:

Enable the command which debug the binding information of DHCPv6 Snooping.

```
switch# debug ipv6 dhcp snooping binding
%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Do binding info from client 00-19-e0-3f-d1-83,
```

```
        interface Ethernet4/11, type 1, transaction-ID 3873
%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Create new binding.
%Jan 16 02:25:14 2006 DHCP6SNP BINDING: Do binding info from client 00-00-00-11-22-33,
        interface Ethernet1/2, type 2, transaction-ID 3873
%Jan 16 02:25:14 2006 DHCP6SNP BINDING: release binding :: MAC 00-19-e0-3f-d1-83 on
default Ethernet4/11
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Do binding info from client 00-19-e0-3f-d1-83,
        interface Ethernet4/11, type 3, transaction-ID 30305
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Create new binding.
%Jan 16 02:25:16 2006 DHCP6SNP BINDING: Do binding info from client 00-00-00-11-22-33,
        interface Ethernet1/2, type 7, transaction-ID 30305
```

28.3 debug ipv6 dhcp snooping event

Command:

debug ipv6 dhcp snooping event

Function:

Debug the event information of DHCPv6 Snooping.

Parameter:

None

Command Mode:

Admin mode

Default:

None

Usage Guide:

Enable this command to show the processing information of the events for DHCPv6 Snooping, the event include sending/deleting the security policy events, such as: black hole MAC, port shutdown/no shutdown, and the error prompt, etc.

Example:

Enable debug of events information for DHCPv6 Snooping.

```
switch# debug ipv6 dhcp snooping event
%Jan 16 02:25:14 2006 DHCP6SNP EVENT: add blackhole 00-19-e0-3f-d1-83 on interface
Ethernet1/13
%Jan 16 02:35:15 2006 DHCP6SNP EVENT: delete blackhole 00-19-e0-3f-d1-83 on interface
Ethernet1/13
```

28.4 debug ipv6 dhcp snooping packet

Command:

debug ipv6 dhcp snooping packet

Function:

Debug the packet information of DHCPv6 Snooping.

Parameter:

None

Command Mode:

Admin mode

Default:

None

Usage Guide:

The processing information of DHCPv6 Snooping packets include the type of the receiving packets, the source MAC and the destination MAC of the packets, client DUID, IA address, preferred lifetime, valid lifetime, and packets drop, etc.

Example:

Enable debug of the packet information for DHCPv6 Snooping.

```
switch# debug ipv6 dhcp snooping packet
%Jan 16 02:18:01 2006 DHCP6SNP EVENT: Parse packet SOLICIT from fe80::219:e0ff:fe3f:d183
    src MAC 00-19-e0-3f-d1-83 interface Ethernet4/11 vlan 1
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from fe80::219:e0ff:fe3f:d183
        src MAC 00-19-e0-3f-d1-83, dst MAC 33-33-00-01-00-02,
        interface Ethernet4/11 vlan 1,
        transaction-ID 2469, smac host flag 0, dmac host flag 0
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x819)
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: to vlan 1 except port Ethernet4/11 (designPort flag 0)
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: and return packet to network stack
%Jan 16 02:18:01 2006 DHCP6SNP EVENT: Parse packet ADVERTISE from fe80::200:ff:fe11:2233
    src MAC 00-00-00-11-22-33 interface Ethernet1/2 vlan 1
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Receive DHCPv6 packet ADVERTISE from fe80::200:ff:fe11:2233
        src MAC 00-00-00-11-22-33, dst MAC 00-19-e0-3f-d1-83,
        interface Ethernet1/2 vlan 1,
        transaction-ID 2469, smac host flag 1, dmac host flag 0
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: Forward packet ADVERTISE (protocol 0x819)
%Jan 16 02:18:01 2006 DHCP6SNP PACKET: to exact port Ethernet4/11 (designPort flag 1)
%Jan 16 02:18:03 2006 DHCP6SNP EVENT: Parse packet REQUEST from fe80::219:e0ff:fe3f:d183
    src MAC 00-19-e0-3f-d1-83 interface Ethernet4/11 vlan 1
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Receive DHCPv6 packet REQUEST from fe80::219:e0ff:fe3f:d183
        src MAC 00-19-e0-3f-d1-83, dst MAC 33-33-00-01-00-02,
        interface Ethernet4/11 vlan 1,
        transaction-ID 16424, smac host flag 0, dmac host flag 0
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Forward packet REQUEST (protocol 0x819)
```

```
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: to vlan 1 except port Ethernet4/11 (designPort flag 0)
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: and return packet to network stack
%Jan 16 02:18:03 2006 DHCP6SNP EVENT: Parse packet REPLY from fe80::200:ff:fe11:2233
      src MAC 00-00-00-11-22-33 interface Ethernet1/2 vlan 1
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Receive DHCPv6 packet REPLY from fe80::200:ff:fe11:2233
            src MAC 00-00-00-11-22-33, dst MAC 00-19-e0-3f-d1-83,
            interface Ethernet1/2 vlan 1,
            transaction-ID 16424, smac host flag 1, dmac host flag 0
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: Forward packet REPLY (protocol 0x819)
%Jan 16 02:18:03 2006 DHCP6SNP PACKET: to exact port Ethernet4/11 (designPort flag 1)
```

28.5 ipv6 dhcp snooping action

Command:

ipv6 dhcp snooping action {shutdown | blackhole} [recovery <*second*>]

no ipv6 dhcp snooping action

Function:

After the abnormity is detected by DHCPv6 Snooping, set the action and the duration on the port, the no command cancels the configuration.

Parameters:

shutdown | blackhole: After DHCPv6 Snooping receives the response packet of DHCPv6 from non-trusted port, then execute the action.

second: The duration between the action execution and recovery , ranging from 1-3600, and the default action is not recovered.

Command Mode:

Port mode

Default Settings:

There is no user-defined action, the default action is not recovered and has no recovery time.

Usage Guide:

Set the user-defined action for non-trusted port, when the security policy is changed, clear the security policy sent to the hardware at the same time.

Example:

Set the user-defined action for non-trusted port.

```
switch(config-if-ethernet1/1)# ipv6 dhcp snooping action shutdown recovery 100
```

28.6 ipv6 dhcp snooping action MaxNum

Command:

ipv6 dhcp snooping action {<*max-num*> | default}

Function:

After the abnormity is detected by DHCPv6 Snooping, set the max number of blackhole MAC on each non-trusted port.

Parameters:

max-num: The max number of blackhole MAC that can be sent after DHCPv6 Snooping receives the response packet of DHCPv6 from non-trusted port, the range from 1 to 200.

default: The limitation number is 10 by default.

Command Mode:

Global mode

Default Settings:

Limit blackhole MAC as 10 by the default port.

Usage Guide:

Set the max number of the blackhole MAC to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is bigger than the setting value, then the earliest blackhole MAC will be recovered forcibly while the new blackhole MAC take effect.

Example:

After the abnormity is detected by DHCPv6 Snooping, set the max number of blackhole MAC as 100 on each non-trusted port.

```
switch(config)# ipv6 dhcp snooping action 100
```

28.7 ipv6 dhcp snooping binding enable

Command:

ipv6 dhcp snooping binding enable

no ipv6 dhcp snooping binding enable

Function:

Enable the DHCPv6 Snooping binding funciton globally. The no command disables the function.

Parameters:

None.

Command Mode:

Globe mode

Default Settings:

DHCPv6 Snooping binding is disabled by default.

Usage Guide:

When enabling the binding function of DHCPv6 Snooping to monitor the DHCPv6 packets, it allows DHCPv6 Snooping binding to be established. This command limits the dynamic binding and the static binding. After disable the global DHCPv6 Snooping function, the device stops establishing the binding according to DHCPv6 packets.

Example:

Establish DHCPv6 Snooping binding according to DHCPv6 REPLY packets.

```
switch(config)#ipv6 dhcp snooping binding enable
```

28.8 ipv6 dhcp snooping binding nd

Command:

ipv6 dhcp snooping binding nd

no ipv6 dhcp snooping binding nd

Function:

Globally enable the function that DHCPv6 Snooping binds ND. The no command disables the function.

Parameters:

None.

Command Mode:

Globe mode

Default Settings:

Disable the function that DHCPv6 Snooping binds ND.

Usage Guide:

After this function is enabled globally, send static ND while setting up DHCPv6 Snooping binding, and convert the already existent DHCPv6 Snooping binding into the static ND entry. After disable the global DHCPv6 Snooping function, the static ND entries will not be set according to DHCPv6 Snooping binding, and all the corresponding static ND entries set by DHCP Snooping binding will be deleted.

Example:

Send the static ND entries according to DHCPv6 Snooping binding.

```
switch(config)#ipv6 dhcp snooping binding nd
```

28.9 ipv6 dhcp snooping binding user

Command:

ipv6 dhcp snooping binding user mac <*MAC-address*> address <*ipv6-address*> vlan <*vid*> interface [ethernet | port-channel] <*ifname*>

no ipv6 dhcp snooping binding user mac <*MAC-address*>

Function:

Users set the static binding entries. The no command deletes the list entry.

Parameters:

MAC-address: The MAC address

vid: VLAN ID, the range from 1 to 4094

ipv6-address: The IPv6 address

ifname: The access interface of the static binding user.

Command Mode:

Globe mode

Default Settings:

There is no static list entry.

Usage Guide:

Add the static list entry to the binding table. For DHCPv6 Snooping binding data, MAC address and IPv6 address must ensure that have no conflict. The static binding data can cover the dynamic binding data and can not be covered by the dynamic binding data.

Port name can the name of a Port-Channel or a Ethernet port, allows the inexistent Port-Channel specified, but it must authenticate the validity of Port-Channel name and can not configure the Ethernet port which is not existent.

In addition, check the validity of MAC and Ipv6 address. MAC must configures the unicast MAC, IPv6 address can not be link local address, loopback address, :: address and multicast address. If the port name exist,,it is still necessary to check whether this port in the vid specified VLAN .

After enable DHCPv6 Snooping and DHCPv6 Snooping binding, the static binding command is able to set.

Example:

Set up the static binding of DHCPv6 Snooping.

```
switch(config)#ipv6 dhcp snooping binding user mac 00-30-4f-01-02-03 address 2010::10 vlan 10 interface ethernet 1/13
```

28.10 ipv6 dhcp snooping binding user-control

Command:

ipv6 dhcp snooping binding user-control

no ipv6 dhcp snooping binding user-control

Function:

Enable the DHCPv6 Snooping binding user-access-control funtion. The no command disables the function.

Parameters:

None.

Command Mode:

Layer 2 port mode

Default Settings:

Disable the DHCPv6 Snooping binding user-access-control.

Usage Guide:

Only enable the global DHCPv6 Snooping function at first, it is able to enable the user-access-control function. This command can not be configured under Port-Channel mode. The no command clears all user-access-control rules of DHCPv6 Snooping on the port, but the binding can not be deleted.

Example:

Enable the user-access-control funtion which is bound by DHCPv6 Snooping.

```
switch(config-if-ethernet1/1)# ipv6 dhcp snooping binding user-control
```

28.11 ipv6 dhcp snooping binding-limit

Command:

ipv6 dhcp snooping binding-limit <*max-num*>

no ipv6 dhcp snooping binding-limit

Function:

Set the max dynamic binding number which is allowed to be set on the port for DHCPv6 Snooping. The no command will not limit the number on the port.

Parameters: max-num:

The max dynamic binding number that port allows to set, and the range from 1 to 100.

Command Mode:

Port mode

Default Settings:

There is no limitation by default.

Usage Guide:

When the limitation number is modified to a smaller value, the redundant dynamic binding will be deleted (delete the aged and interim binding at first). The static binding, which is created by user configuration, is not limited in number.

Example:

Set the allowed max dynamic binding number as 10.

```
switch(config-if-ethernet1/1)# ipv6 dhcp snooping binding-limit 10
```

28.12 ipv6 dhcp snooping enable

Command:

ipv6 dhcp snooping enable

no ipv6 dhcp snooping enable

Function:

Enable DHCPv6 Snooping globally. The no command disables the function.

Parameters:

None.

Command Mode:

Globe mode

Default Settings:

Disable DHCPv6 Snooping.

Usage Guide:

After enable the DHCPv6 Snooping function globally, it is possible for the DHCPv6 Snooping to be configured in a port, the DHCPv6 packets of all ports can not be forwarded directly and are copied to cpu to be processed and forwarded by DHCPv6 Snooping. After disable the global DHCPv6 Snooping function and all ports functions of DHCPv6 Snooping, the DHCPv6 packets are forwarded directly and do not need to be copied to cpu, so DHCPv6 Snooping will not process DHCPv6 packets any more.

Example:

Enable the monitor function of DHCPv6 Snooping globally.

```
switch(config)#ipv6 dhcp snooping enable
```

28.13 ip dhcp snooping trust

Command:

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Function:

Set the port to the trusted port. The no command sets the port to non-trusted port.

Parameters:

None

Command Mode:

Port mode

Default Settings:

By default, the port is non-trusted port.

Usage Guide:

When a port turns into a trusted port from a non-trusted port, the original security policy of the port will be deleted that means clear all blackhole MAC or undo the shutdown of this port. At the same time, it allows the DHCPv6 responding packets of this port to be forwarded. When a port turns into a non-trusted port from a trusted port, forbid the DHCPv6 responding packets to be forwarded and drop them.

Example:

Set the port as the trusted port.

```
switch(config-if-ethernet1/1)# ipv6 dhcp snooping trust
```

28.14 show ipv6 dhcp snooping

Command:

show ipv6 dhcp snooping

Function:

Display the current global cofiguration of DHCPv6 Snooping.

Parameters:

None.

Command Mode:

Any Mode.

Default Settings:

None.

Usage Guide:

Collect the information: the global switch, the trusted attributes of each port, the binding information number of ports, the warning information number (security policy number) of the ports, etc.

Example:

Display the current global cofiguration of DHCPv6 Snooping.

```
switch(config)# show ipv6 dhcp snooping
DHCPv6 Snooping is enabled

DHCPv6 Snooping maxnum of action info:10
```

```
switch ID: 00-30-4f-dc-dc-dc
DHCPv6 Snooping discarded packets: 0
DHCPv6 Snooping alarm count: 0, binding count: 0,
   static binding count 0,
   dynamic binding count: 0
Message: SOLICIT number: 0
Message: ADVERTISE number: 0
Message: REQUEST number: 0
Message: CONFIRM number: 0
Message: RENEW number: 0
Message: REBIND number: 0
Message: REPLY number: 0
Message: RELEASE number: 0
Message: DECLINE number: 0
Message: RECONFIGURE number: 0
Message: INFORMATION REQUEST number: 0
Message: RELAY-FORWARD number: 0
Message: RELAY-REPLY number: 0

interface          trust         action       recovery     alarm num    bind num
---------------- ---------- ---------- ---------- ---------- ----------
Ethernet1/1        trust         none          0              0              0
Ethernet1/2        untrust       none          0              0              0
Ethernet1/3        untrust       none          0              0              0
Ethernet1/4        untrust       none          0              0              0
Ethernet1/5        untrust       none          0              0              0
Ethernet1/6        untrust       none          0              0              0
Ethernet1/7        untrust       none          0              0              0
Ethernet1/8        untrust       none          0              0              0
Ethernet1/9        untrust       none          0              0              0
Ethernet1/10       untrust       none          0              0              0
Ethernet1/11       untrust       none          0              0              0
Ethernet1/12       untrust       none          0              0              0
Ethernet1/13       untrust       none          0              0              0
Ethernet1/14       untrust       none          0              0              0
Ethernet1/15       untrust       none          0              0              0
Ethernet1/16       untrust       none          0              0              0
Ethernet1/17       untrust       none          0              0              0
Ethernet1/18       untrust       none          0              0              0
Ethernet1/19       untrust       none          0              0              0
Ethernet1/20       untrust       none          0              0              0
Ethernet1/21       untrust       none          0              0              0
Ethernet1/22       untrust       none          0              0              0
Ethernet1/23       untrust       none          0              0              0
```

Ethernet1/24	untrust	none	0	0	0
Ethernet1/25	untrust	none	0	0	0
Ethernet1/26	untrust	none	0	0	0
Ethernet1/27	untrust	none	0	0	0
Ethernet1/28	untrust	none	0	0	0

28.15 show ipv6 dhcp snooping binding

Command:

show ipv6 dhcp snooping binding {<*MAC*> | <*ipv6-address*> | interface {ethernet <*IFNAME*> | <*IFNAME*>} | all}

Function:

Show the binding information of DHCPv6 Snooping.

Parameter:

MAC: Show the specific MAC address

ipv6 address: Show the specific IPv6 address

IFNAME: The port ID

all: Show all DHCPv6 Snooping binding

Command Mode:

Any mode

Default:

None

Usage Guide:

Display the specified (one port or all ports) binding information for DHCPv6 Snooping.

Example:

Disable the binding information function of DHCPv6 Snooping:

```
switch(config)# show ipv6 dhcp snooping binding all
DHCPv6 Snooping is enabled

DHCPv6 Snooping binding count 1, static binding 0

MAC                        IPv6 address    Interface          Vlan ID      State
-------------------------------------------------------------------------------------------------------------------00-19-e0-3f-d1-83
2001::100        Ethernet1/13     1              DHCPv6_BOUND
```

28.16 show ipv6 dhcp snooping interface

Command:

show ipv6 dhcp snooping interface <szIfName>

Function:

Display the current port cofiguration of DHCPv6 Snooping.

Parameters: .szIfName:

The port name.

Command Mode:

Any Mode.

Default Settings:

None.

Usage Guide:

Collect the information about the ports: the relating configuration, the detail information of binding data, detail information of the warning data.

Example:

Display the current port cofiguration of DHCPv6 Snooping.

```
switch(config)# show ipv6 dhcp snooping interface ethernet 1/13
interface Ethernet1/13 user config:
trust attribute: untrust
action: none
binding user control: disabled
recovery interval: infinite
Alarm info: 0

Dynamic binding info: 1
------------------------------------------------------------
DHCPv6 Snooping Binding built at MON JAN 16 02:40:29 2006
        Time Stamp: 5634
        Vlan: 1, Port: Ethernet1/13
        Client MAC: 00-19-e0-3f-d1-83
        Client IPv6 addr: 2001::200
        Lease: 259200(s)
        Flag: Dynamic
Static Binding info: 0
```

Chapter 29 Commands for Routing Policy

29.1 ip prefix-list description

Command:

ip prefix-list <*list_name*> description <*description*>

no ip prefix-list <*list_name*> description

Function:

Configure the description of the prefix-list. The "**no ip prefix-list <*list_name*> description**" command deletes the description contents.

Parameter:

<list _name> is the name of the prefix-list,

<description >is the description contents.

Default:

None.

Command Mode:

Global Mode

Usage Guide:

This command can be used for explaining and describing a prefix-list, e.g. the application and attention matters of the prefix-list.

Example:

Switch#config terminal
Switch(config)#ip prefix-list 3 description This list is used by BGP

29.2 ip prefix-list seq

Command:

ip prefix-list <*list_name*> [seq <*sequence_number*>] <deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>

no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]

Function:

Configure the prefix-list. The "**no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]**" command deletes the prefix-list.

Parameter:

<list _name> is the name of prefix-list, "seq" shows the following parameters is the sequence number, ***<sequence_number>*** is the sequence number, "deny" means deny this route, "permit" means permit this route, "any" means adaptive to all packets with any prefix as well as any mask length, ***ip_addr/mask_length*** shows the prefix address (dotted decimal notation) and the length of mask, "ge" means greater than or equal to, ***<min_prefix_len>*** is the minimum length of prefix to

be matched（ranging between 0～32）, “le” means less than or equal to, ***<max_prefix_len>*** is the maximum length of prefix to be matched（ranging between 0～32）.

Default:

None.

Command Mode:

Global Mode

Usage Guide:

A prefix-list is identified by a prefix-list name. Each prefix-list may include several items each of which independently specifies a matching scope of network prefix-list type which is identified with a *sequence-number. sequence-number* specifies the sequence of matching check in the prefix-list. In the matching process the switch check in turn every items identified by “*sequence-number*” ascending. Once certain item obtains the conditions then the prefix-list filter is passed (without proceeding into the next item check)

Attentions should be paid on that at least one item match mode should be “permit” when more than one prefix-list items is defined. The deny mode items can be previously defined so to remove the unsuitable routing messages fast. However if all items are at deny mode then none of the routes would be able to pass the filter of this prefix-list. We here can define a “permit 0.0.0.0/0 ge 0 le 32” item after several defined “deny mode” items so to grant the passage for all other routing messages.

Example:

```
Switch#config terminal
```

```
Switch(config)#ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14
```

29.3 ip prefix-list sequence-number

Command:

ip prefix-list sequence-number

no ip prefix-list sequence-number

Function:

Enable the sequence-number auto-creation function, the “**no ip prefix-list sequence-number**” command close the prefix-list sequence-number.

Parameter:

None.

Default:

Sequence-number auto-creation enabled.

Command Mode:

Global Mode

Usage Guide:

The command can be used to close the prefix-list sequence-number.

Example:

```
Switch(config)#no ip prefix-list sequence-number
```

29.4 match as-path

Command:

match as-path <*list-name*>

no match as-path [<*list-name*>]

Function:

Configure the AS path domain for matching the BGP routing messages. The "**no match as-path [<*list-name*>]**"delete this configuration.

Parameter:

<list-name > is the name of access-list.

Command Mode:

route-map mode

Usage Guide:

This command matches the AS path domain of the BGP routing message following the rules specified in the as-path list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match as-path 60

29.5 match community

Command:

match community <*community-list-name* | *community-list-num* > [exact-match]

no match community [<*community-list-name* | *community-list-num* > [exact-match]]

Function:

Configure the community attributes of BGP routing messages. The "**no match community [<*community-list-name* | *community-list-num* > [exact-match]]**" command deletes this configuration.

Parameter:

***<community-list-name* >** is the name of the community-list, ***<community-list-num* >** is the community-list sequence number, ranging between 1～99（Standard ACL）or 100～199（Extended ACL）, **[exact-match]** means precise matching.

Command Mode:

route-map mode

Usage Guide:

This command matches the community attributes of the BGP routing message following the rules specified in the community list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match community 100 exact-match

29.6 match interface

Command:

match interface <*interface-name*e >

no match interface [<*interface-name*e >]

Function:

Configure to match the interfaces. The "**no match interface [<*interface-name*e >]**"deletes this configuration.

Parameter:

"***<interface-name >***"is the name of the interface.

Command Mode:

route-map mode

Usage Guide:

This command matches according to the next-hop messages in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed. This command is only used in RIP and OSPF protocols.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match interface vlan1

29.7 match ip

Command:

match ip <address | next-hop> <*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>

no match ip <address | next-hop> [<*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>]

Function:

Configure the routing prefix or next-hop. The "**no match ip <*address* | *next-hop*> [<*ip-acl -name* | *ip-acl -num* | prefix-list *list-name*>]**" deletes this configuration.

Parameter:

<address > means matching the routing prefix, **<next-hop>**means matching the routing next-hop, ***<ip-acl -name >*** is the name of ip access-list, ***<ip-acl -num >*** is the ip access-list sequence number, ranging between 1～199 or 1300～2699（extension scope）, **prefix-list** means the matching should follow the prefix-list rules, ***list-name*** is the name of prefix-list.

Command Mode:

route-map mode

Usage Guide:

This command matches according to the next-hop messages or routing prefix in the route. If the matching succeeded, then the “permit” or “deny” action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match ip address prefix-list mylist

29.8 match ipv6 address

Command:

match ipv6 address <*ipv6-acl-name* | *prefix-list list-name*>

no match ipv6 address [<*ipv6-acl-name* | *prefix-list list-name*>]

Function:

Configure the prefix for ipv6 routing. If the no form command is enaled, the configuration will be removed.

Parameters:

address is the routing prefix to be matched. **<ipv6-acl-name>** is the name of ipv6 access list. Or when the **prefix-list** is configured. **list-name** will be the list name to be matched.

Command Mode:

route map mode

Usage Guide:

When this command is enabled, the prefix-list in the routing table will be used for routing decision. And if matched, the permit deny operation in the route map will be executed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match ipv6 address prefix-list mylist

29.9 match ipv6 next-hop

Command:

match ipv6 next-hop <*ipv6-address*>

no match ipv6 next-hop [<*ipv6-address*>]

Function:

Configure the next hop for ipv6 routing. The no form command will disable the configuration.

Parameters:

next-hop is the next station for routing. ipv6-address is the ipv6 address for the ip address of the interface on the next station.

Command Mode:

route map mode

Usage Guide:

If this command is configured, packets will be delivered according to the next hop information in the routing table. If matched, the permit or deny operation in the route map will be executed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)# match ipv6 next-hop 2000::1

29.10 match metric

Command:

match metric <*metric-val* >

no match metric [<*metric-val* >]

Function:

Match the metric value in the routing message. The "**no match metric [<*metric-val* >]**" deletes the configuration.

Parameter:

<metric-val > is the metric value, ranging between 0～4294967295.

Command Mode:

route-map mode

Usage Guide:

This command matches according to metric value in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match metric 60

29.11 match origin

Command:

match origin <egp | igp | incomplete >

no match origin <egp | igp | incomplete >

Function:

Configure to matching with the origin of the BGP routing message. The "**no match origin <egp | igp | incomplete >**"deletes the configuration.

Parameter:

egp means the route is learnt from the external gateway protocols, **igp** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode:

route-map mode

Usage Guide:

This command matches according to origin message in the BGP route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match origin egp

29.12 match route-type

Command:

match route-type external <type-1 | type-2 >

no match route-type external [<type-1 | type-2 >]

Function:

Configure to matching with the route type of OSPF routing message. The "**no match route-type external [<type-1 | type-2 >]**" deletes the configuration.

Parameter:

type-1 means match with the OSPF type 1 external route, **type-2** means match with the OSPF type 2 external route.

Command Mode:

route-map mode

Usage Guide:

This command matches according to the type of OSPF routes （OSPF AS-external LSA type is either type 1 or type 2）. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match route-type external type-1

29.13 match tag

Command:

match tag <*tag-val* >

no match tag [<*tag-val* >]

Function:

Configure to matching with the tag domain of the OSPF routing message. The "**no match tag [<*tag-val* >]**" deletes this configuration.

Parameter:

<*tag-val* > is the tag value, ranging between 0～4294967295.

Command Mode:

route-map mode

Usage Guide:

This command matches according to the tag value in the OSPF route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match tag 60

29.14 route-map

Command:

route-map <*map_name*> {deny | permit} <*sequence_num*>

no route-map <*map_name*> [{deny | permit} <*sequence_num*>]

Function:

Configure the route-map and entering the route-map mode. The "**no route-map <*map_name*> [{deny | permit} <*sequence_num*>]**" command deletes route-map.

Parameter:

<*map_name*> is the name of route-map, **permit** sets route-map matching mode to permit mode, **deny** sets route-map matching mode to permit mode（**set** sub will not be executed under this mode）, **<*sequence_num*>** is the route-map sequence number, ranging between 1～65535.

Default:

None

Command Mode:

Global Mode

Usage Guide:

A route-map may consist of several nodes each of which is a check unit. The check sequence among nodes is identified by *sequence-number*. “permit” means the node filter will be passed if all match subs are obtained by current route and then further all the set sub of this node will be executed without entering the check in the next node; if the match subs can not be met, the proceed to the check in next node. Relation among different node should be “or”, namely one node check passed then the route filter is passed when the switch checks each node in turn in the route-map.

Attentions should be paid on that at least one node match mode should be “permit” when more than one node is defined. When a route-map is used for filtering routing messages, if certain routing message can not pass any node check, then it is considered denied by the route-map. If all nodes in the route-map are set to deny mode, then all routing message should not be able to pass that route-map.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match as-path 60
Switch(config-route-map)#set weight 30

29.15 set aggregator

Command:

set aggregator as <*as-number*> <*ip_addr*>

no set aggregator as [<*as-number*> <*ip_addr*>]

Function:

Assign an AS number for BGP aggregator. The “**no set aggregator as [<*as-number*> <*ip_addr*>]**” deletes this configuration.

Parameter:

<as-number > is the AS number, ***<ip_addr>*** is the ip address of the aggregator shown in decimal notation.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set aggregator as 200 10.1.1.1

29.16 set as-path

Command:

set as-path prepend <*as-num*>

no set as-path prepend [<*as-num*>]

Function:

Add AS numbers in the AS path domain of the BGP routing message. The "**no set as-path prepend [<*as-num*>]**" command deletes this configuration.

Parameter:

<as-num > is the AS number, circulating inputting several numbers is available.

Command Mode:

route-map mode

Usage Guide:

To add AS number in the As domain of the BGP, the AS path length should be lengthened so to affect the best neighbor path option. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set as-path prepend 200

29.17 set atomic-aggregate

Command:

set atomic-aggregate

no set atomic-aggregate

Function:

Configure the atomic aggregate attributes. The "**no set atomic-aggregate**" command deletes this configuration.

Parameter:

None

Command Mode:

route-map mode

Usage Guide:

The BGP informs other BGP speaker by the atomic aggregate attributes. Local system selects a sub-specified route other than the more specified routes included in it. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5

```
Switch(config-route-map)#set atomic-aggregate
```

29.18 set comm-list

Command:

set comm-list <*community-list-name* | *community-list-num* > delete

no set comm-list <*community-list-name* | *community-list-num* > delete

Function:

Configure to delete the community attributes from the inbound or outbound routing messages. The "**no set comm-list <*community-list-name* | *community-list-num* > delete**" command deletes the configuration.

Parameter:

***<community-list-name* >** is the name of community list, ***<community-list-num* >** is the sequence number of community list, ranging between 1～99（standard community list） or 100～19（extended community list）.

Command Mode:

route-map mode

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set comm-list 100 delete
```

29.19 set community

Command:

set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

Function:

Configure the community attributes of the BGP routing message. The "**no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**" command deletes this configuration.

Parameter:

[*AA:NN*] is the community attribute value, **[internet]** is the internet scope, **[local-AS]** means this route do not announce outside the local AS (but can announce among the sub AS within the confederation), **[no-advertise]** means this route do not send to any neighbor, **[no-export]** means this route do not send to EBGP neighbors, **[none]** means delete the community attributes from the prefix of this route, **[additive]** means add following existing community attributes.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set community local-as additive

29.20 set extcommunity

Command:

set extcommunity <rt | soo> <*AA:NN*>

no set extcommunity <rt | soo> [<*AA:NN*>]

Function:

Configure the extended community attributes of the BGP routing message. The "**no set extcommunity <rt | soo> [<*AA:NN*>]**" command deletes this configuration.

Parameter:

<rt> is the route target, ***<soo>*** is the site of origin, ***<AA:NN>*** is the value of community attributes, amongst AA is AS number, NN is a random two byte number.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set extcommunity rt 100:10

29.21 set ip next-hop

Command:

set ip next-hop <*ip_addr*>

no set ip next-hop [<*ip_addr*>]

Function:

Configure the next-hop of the route. The "**no set ip next-hop [<*ip_addr*>]**" command deletes the configuration.

Parameter:

<ip_addr > is the ip address of next-hop shown with dotted decimal notation.

Command Mode:

route-map mode

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set ip next-hop 10.2.2.2

29.22 set local-preference

Command:

set local-preference <*pre_val*>

no set local-preference [<*pre_val*>]

Function:

Configure the local priority of BGP route. The "**no set local-preference [<*pre_val*>]**" command deletes this configuration.

Parameter:

<pre_val > is the value of local priority, ranging between 0～4294967295.

Command Mode:

route-map mode

Usage Guide:

The local priority attribute is the priority level of a route. A route with a higher local priority level when compared with other route of the same destination, will be more preferred than other route. The local priority validates only within this AS and will not be transported to EBGP neighbors. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set local-preference 60

29.23 set metric

Command:

set metric < *metric_val*>

no set metric [< *metric_val*>]

Function:

Configure the metric value of the route. The "**no set metric [< *metric_val*>]**" command deletes the configuration.

Parameter:

<metric_val > is the metric value, ranging between 1～4294967295.

Command Mode:

route-map mode

Usage Guide:

The metric value only affects the path option from external neighbors to local AS. The less the metric value is the higher is the priority. Under normal circumstances only the path metric value of the neighbors of the same AS will be compared. To extend the comparison to the metric values of different neighbor path, the bgp always-compare-med command should be configured. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set metric 60

29.24 set metric-type

Command:

set metric-type <type-1 | type-2>

no set metric-type [<type-1 | type-2>]

Function:

Configure the metric type of the OSPF routing message. The "**no set metric-type [<type-1 | type-2>]**" command deletes this configuration.

Parameter:

type-1 means matches the OSPF type 1 external route, **type-2** means matches the OSPF type 2 external route.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set metric-type type-1

29.25 set origin

Command:

set origin <egp | igp | incomplete >

no set origin [<egp | igp | incomplete >]

Function:

Configure the origin code of the BGP routing message. The "**no set origin [<egp | igp | incomplete >]**" command deletes this configuration.

Parameter:

egp means the route is learnt from the external gateway protocols, **igp** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set origin egp

29.26 set originator-id

Command:

set originator-id <*ip_addr*>

no set originator-id [<*ip_addr*>]

Function:

Configure the origin ip address of the BGP routing message. The "**no set originator-id [<*ip_addr*>]**" command deletes the configuration.

Parameter:

<ip_addr> is the ip address of the route source shown by dotted decimal notation.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set originator-id 10.1.1.1

29.27 set tag

Command:

set tag <*tag_val*>

no set tag [<*tag_val*>]

Function:

Configure the tag domain of OSPF routing messages. The "**no set tag [<*tag_val*>]**" command deletes this configuration.

Parameter:

<tag-val > is the tag value, ranging between 0～4294967295.

Command Mode:

route-map mode

Usage Guide:

There is a route-tag domain at the AS-external-LSA type LSA. The domain is normally identified by other routing protocols. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set tag 60

29.28 set vpnv4 next-hop

Command:

set vpnv4 next-hop <*ip_addr*>

no set vpnv4 next-hop [<*ip_addr*>]

Function:

Configure the next-hop of BGP VPNv4 routing message. The "**no set vpnv4 next-hop [<*ip_addr*>]**" command deletes the configuration.

Parameter:

<ip_addr> is the next-hop ip address of VPNv4 route shown by dotted decimal notation.

Command Mode:

route-map mode

Usage Guide:

To use this command, one match clause should at first be defined.

Example:

Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set vpnv4 next-hop 10.1.1.1

29.29 set weight

Command:

set weight <*weight_val*>

no set weight [<*weight_val*>]

Function:

Configure the weight value of BGP routing message. The "**no set weight [<*weight_val*>]**" command deletes this configuration.

Parameter:

<weight_val> is weight value, ranging between 0～4294967295

Command Mode:

route-map mode

Usage Guide:

Weight value is adopted to facilitate the best path option and validates only within the local switch. While there are several route to the same destination the one with higher priority is more preferred. To use this command, one match clause should at first be defined.

Example:

```
Switch#config terminal
```

```
Switch(config)#route-map r1 permit 5
```

```
Switch(config-route-map)#set weight 60
```

29.30 show ip prefix-list <list-name>

Command:

show ip prefix-list [*<list-name>* [*<ip_addr/len>* [first-match | longer] | seq *<sequence-number>*]]

Function:

Show by prefix-list names.

Parameter:

<list-name> is the name of prefix-list, ***<ip_addr/len>*** is the prefix ip address and the length of mask, **first-match** stands for the first route table matched with specified ip address, **longer** means longer prefix is required, **seq** means show by sequence number, ***<sequence-number>*** is the sequence number, ranging between 0～4294967295.

Default:

None

Command Mode:

Admin mode

Usage Guide:

All prefix-list will be listed when no prefix-list name is specified.

Example:

```
Switch#show ip prefix-list
ip prefix-list 1: 1 entries
    deny any
ip prefix-list mylist: 1 entries
    deny 1.1.1.1/8
```

```
Switch#show ip prefix-list mylist 1.1.1.1/8
    seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)
```

Displayed information Explanation
ip prefix-list mylist: 1 entries Show a prefix-list named mylist which includes 1 instance.
seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0) Show the prefix-list contents sequence numbered 5. hit count: 0 means being hit 0 time, recount: 0 means referred 0 time.

29.31 show ip prefix-list<detail|summary>

Command:

show ip prefix-list [<detail | summary> [<*list-name*>]]

Function:

Display the contents of the prefix list.

Parameters:

When **detail** is enabled, detail of prefix-list will be displayed. For **summary**, it is similar but a summary will be displayed. ***<list-name>*** is the name of the prefix list.

Default:

None.

Command Mode:

Privileged mode and configuration mode

Usage Guide:

If no prefix list name is specified, all the prefix list will be displayed.

Example:

Switch#show ip prefix-list detail mylist ip prefix-list mylist: count: 2, range entries: 0, sequences: 5 - 10 seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0) seq 10 permit 2.2.2.2/8 (hit count: 0, refcount: 0)
Switch#show ip prefix-list summary mylist ip prefix-list mylist: count: 2, range entries: 0, sequences: 5 – 10

Displayed information Explanation

ip prefix-list mylist: To display the prefix list which named mylist.
count: 2, range entries: 0, sequences: 5 - 10 count : 2 means there are two prefix list instances. sequences: 5-10 means the sequence number. 5 is the starting sequence number, while 10 is the ending.
deny 1.1.1.1/8 (hit count: 0, refcount: 0) deny 1.1.1.1/8 is contents of the prefix list. hit count:0 means the rule has been matched for zero times. And refcount:0 means the rule is referenced for zero times.

29.32 show route-map

Command:

show route-map

Function:

Show the content of route-map.

Parameter:

None

Default:

None

Command Mode:

Admin mode

Usage Guide:

None

Example:

```
Switch# show route-map
route-map a, deny, sequence 10
  Match clauses:
    as-path 60
  Set clauses:
    metric 10
```

Displayed information Explanation
route-map a, deny, sequence 10 route-map a means the name of route map is a, deny means the deny mode, sequence 10 means

the sequence number is 10
Match clauses: Match sub
as-path 60 Detailed contents in the Match sub
Set clauses: Set sub
metric 10 Detailed content in the Set clause

29.33 show router-id

Command:

show router-id

Function:

Show the content of router-id.

Parameter:

None

Default:

None

Command Mode:

Admin and Configuration Mode

Usage Guide:

None

Example:

1: Switch#show router-id Router ID: 20.1.1.1 (automatic)
2: Switch#show router-id Router ID: 20.1.1.2 (config)

Chapter 30 Commands for Static Route

30.1 ip route

Command:

ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} {*<gateway-address>* | *<gateway-interface>*} [*<distance>*]

no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]

Function:

Configure the static route. The "**no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]**" command deletes the static route.

Parameter: The ***<ip-prefix>*** and ***<mask>*** are respectively destination IP address and subnet mask, shown in dotted decimal notation; ***<ip-prefix>*** and ***<prefix-length>*** are respectively the destination IP address and the length of prefix; ***<gateway-address>*** is the next-hop IP address shown in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface, ***< distance >*** is the manage distance of route management, ranging between 1～255.

Default:

The management distance of static routing is defaulted at 1.

Command Mode:

Global Mode.

Usage Guide:

When configuring the next-hop of static routing, both by specifying the next-hop IP address of the route data packet and the exit interface are available.

The default distance values of each route type in the layer 3 switch of our company are listed below:

Route Type Distance Value
Direct Route 0
Static Route 1
OSPF 110
RIP 120
IBGP 200
EBGP 20

The direct route has the highest priority when each route management distance value remain unchanged and followed by static route, EBGP、OSPF、RIP、IBGP.

Example:

Example 1. Add a static route

```
Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1
```

Example 2. Add default route

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1
```

30.2 show ip route

Command:

show ip route [<*destination*>|<*destination* >|<*length*>|connected | static | rip| ospf | bgp | isis| kernel| statistics| database [connected | static | rip| ospf | bgp | isis| kernel] |fib[statistics]]

Function:

Show the route table.

Parameter:

<destination> is the destination network address; ***<destination >/<length>*** is the destination network address plus the length of prefix**; connected** is direct route; **static** is static route; **rip** is RIP route; **ospf** is OSPF route; **bgp** is BGP route; **isis** is ISIS route; **kernel** is kernel route; **statistics** shows the number of routes; **database** is route database; **fib** is kernel route table.

Command Mode:

Admin mode

Usage Guide:

Show all the contents in the route table including: route type, destination network, mask, next-hop address, interface, etc

Example:

```
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
Gateway of last resort is 210.0.0.3 to network 0.0.0.0
S*        0.0.0.0/0 [1/0] via 210.0.0.3, Vlan1
C        127.0.0.0/8 is directly connected, Loopback
O IA     172.16.11.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA     172.16.12.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA     172.16.13.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA     172.16.14.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
```

```
O IA     172.16.15.0/24 [110/50] via 210.14.0.1, Vlan3014, 00:00:47
O E2    172.16.100.0/24 [110/0] via 210.14.0.1, Vlan3014, 00:00:46
```

Displayed information Explanation
C –connected Direct route, namely the segment directly connected with the layer 3 switch
S –static Static route, the route manually configured by users
R - RIP derived RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE Route introduced by OSPF
B- BGP derived BGP route, acquired by the BGP protocol.
Destination Target network
Mask Target network mask
Nexthop Next-hop IP address
Interface Next-hop pass-by layer 3 swtich interfaces
Preference Route priority. If other types of route to the target network exists, the kernel route will only shows those with high priority.

30.3 show ip route vrf

Command:

show ip route vrf <name> [connected | static | rip| ospf | bgp | isis| kernel|statistics|database[connected | static | rip| ospf | bgp | isis|kernel]]

show ip route fib vrf <name> [default|main|local]

Function:

Show the routing tables entries.

Parameters:

<name> is the name of the delivering instance of routing. **<destination>/<length>** are the network address for the destination as well as the length of the network mask. **connected** is for direct routing. **static** is for static routing. **rip** is for the RIP routing protocol. **ospf** is for the OSPF routing protocol. **bgp** is for the BGP routing protocol. **isis** is for the ISIS routing protocol. **kernel** is for the kernel routing protocol. **statistics** are the number of routing entries to be displayed. **database** is for the routing database. **fib** is for the core routing table.

Command Mode:

all modes.

Usage Guide:

To display the contents of the VPN routing table, including routing type, destination network address, address mask, the address and interface for the next hop, etc.

30.4 ip route vrf

Command:

ip route vrf <name> {<ip-prefix> <mask>|<ip-prefix/<prefix-length>} {<gateway-address>|<gateway-interface>} [<distance>]

no ip route vrf <name> {<ip-prefix> <mask>|<ip-prefix/<prefix-length>} [<gateway-address>|<gateway-interface>] [<distance>]

Function:

To configure the static routing. The no form command will disable the command.

Parameters:

<name> is the name of the VPN routing instance. **<ip-prefix>** and **<mask>** are the network address and mask of the destination in dotted decimal format. **<ip-prefix>** and **<prefix-length>** are similar but **<prefix-length>** is the length of the address mask. **<gateway-address>** is the ip address of next hop in dotted decimal format. **<gateway-interface>** is the interface for the next hop. **<distance>** is the weight of the routing entry, which is allowed to value between 1 and 255.

Default:

The distance of the routing entry is 1 by default.

Command Mode:

Global configuration mode.

Usage Guide: VPN routing instance should be configured before this commnad can be issued.

Chapter 31 Commands for RIP

31.1 accept-lifetime

Command:

accept-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no accept-lifetime

Function:

Use this command to specify a key accept on the key chain as a valid time period. The "**no accept-lifetime**" command deletes this configuration.

Parameter:

<start-time> parameter specifies the start time of the time period, of which the form should be:

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> specifies the date of valid, ranging between 1 -31

<month> specifies the month of valid shown with the first three letters of the month, such as Jan

<year> specifies the year of valid start, ranging between 1993 - 2035

<end-time> specifies the due of the time period, of which the form should be:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> specifies the date of valid, ranging between 1 -31

<month> specifies the month of valid shown with the first three letters of the month, such as Jan

<year> specifies the year of valid start, ranging between 1993 - 2035

<seconds> the valid period of the key in seconds, ranging between 1-2147483646

Infinite means the key will never be out of date.

Default:

No default configuration.

Command Mode:

keychain-key mode

Usage Guide:

Refer to the 3.13 RIP authentication Introduction.

Example:

The example below shows the accept-lifetime configuration of key 1 on the keychain named mychain.

Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

Related Command:

key

key-string

key chain

send-lifetime

31.2 address-family ipv4

Command:

address-family ipv4 vrf <*vrf-name*>

no address-family ipv4 vrf <*vrf-name*>

Function:

Configure this command to enable the routing message switching among VRF and enter the address-family mode. The "**no address-family ipv4 vrf <*vrf-name*>**" command deletes the RIP instances related to this VPN routing/forwarding instance.

Parameter:

<vrf-name> specifies the name of VPN routing/forwarding instances.

Command Mode:

router mode

Usage Guide:

This command is only used on PE router. A VPN routing/forwarding instance must be generated with command ip vrf prior to using this command by which the VPN routing/forwarding instances can be related to RIP instances.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VRF1
Switch(config-router-af)#

31.3 clear ip rip route

Command:

clear ip rip route {<*A.B.C.D/M*> | kernel | static | connected | rip | ospf | isis | bgp | all}

Function:

Clear specific route in the RIP route table.

Parameter:

<A.B.C.D/M> Clear the routes which match the destination address from the RIP route table. specifies the IP address prefix and its length of the destination address

kernel delete kernel routes from the RIP route table

static delete static routes from the RIP route table

connected delete direct routes from the RIP route table

rip only delete RIP routes from the RIP route table

ospf only delete OSPF routes from the RIP route table

isis only delete ISIS routes from the RIP route table

bgp only delete BGP routes from the RIP route table

all delete all routes from the RIP route table

Default:

No default configurations.

Command Mode:

Admin mode

Usage Guide:

Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.

Example:

Switch# clear ip rip route 10.0.0.0/8
Switch# clear ip rip route ospf

31.4 debug rip

Command:

debug rip [events| nsm| packet[recv|send][detail]| all]

no debug rip [events| nsm| packet[recv|send][detail]| all]

Function:

Open various RIP adjustment switches and show various adjustment debugging messages. The "**no debug rip [events| nsm| packet[recv|send][detail]| all]**" command close corresponding debugging switch.

Parameter:

events shows the debugging messages of RIP events

nsm shows the communication messages between RIP and NSM

packet shows the debugging messages of RIP data packets

recv shows the messages of the received data packets

send shows the messages of the sent data packets

detail shows the messages of received or sent data packets

Default: Debug switch closed.

Command Mode:

Admin mode and global mode

Example:

Switch# debug rip packet
Switch#1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520 1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520 1970/01/01 01:01:47 IMI: RECV[Vlan1]: Receive from 20.1.1.2:520

31.5 debug rip redistribute message send

Command:

debug rip redistribute message send

no debug rip redistribute message send

Function:

To enable the debugging of sending messages for routing redistribution messages from OSPF process or BGP protocol for RIP. The no form of this command will disable the debugging messages.

Parameter:

None.

Default:

Close the debug by default.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

Switch#debug rip redistribute message send
Switch#no debug rip redistribute message send

31.6 debug rip redistribute route receive

Command:

debug rip redistribute route receive

no debug rip redistribute route receive

Function:

To enable debugging of received messages from NSM for RIP. The no form of this command will disable debugging of received messages from NSM for RIP.

Parameter:

None.

Default:

Close the debug by default.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

Switch#debug rip redistribute route receive
Switch#no debug rip redistribute route receive

31.7 default-information originate

Command:

default-information originate

no default-information originate

Function:

Allow the network 0.0.0.0 to be redistributed into the RIP. The "**no default-information originate**" disable this function.

Parameter:

None

Default:

Disabled

Command Mode:

Router mode and address-family mode

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# default-information originate

31.8 default-metric

Command:

default-metric <*value*>

no default-metric

Function:

Set the default metric value of the introduced route. The "**no default-metric**" command restores the default value to 1.

Parameter:

<value> is the metric value to be set, ranging between 1~16.

Default:

Default route metric value is 1.

Command Mode:

Router mode and address-family mode

Usage Guide:

default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIP routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example:

Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes.

Switch(config-router)#default-metric 3

Relevant Commands:

Redistribute

31.9 distance

Command:

distance <*number*> [<*A.B.C.D/M*>] [<*access-list-name* | *access-list-number* >]

no distance [<*A.B.C.D/M*>]

Function:

Set the managing distance with this command. The "**no distance [<*A.B.C.D/M*>]**" command restores the default value to 120.

Parameter:

<number> specifies the distance value, ranging between 1 to 255.

<A.B.C.D/M> specifies the network prefix and its length.

<access-list-name | access-list-number > specifies the access-list number or name applied.

Default:

The default managing distance of RIP is 120.

Command Mode:

Router mode and address-family mode

Usage Guide:

In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distance 8 10.0.0.0/8 mylist

31.10 distribute-list

Command:

distribute-list {<*access-list-number* | *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

no distribute-list {<*access-list-numbe r*| *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

Function:

This command uses access-list or prefix-list to filter the route update packets sent and received. The "**no distribute-list {<*access-list-number*| *access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]**" command cancels this route filter function.

Parameter:

<access-list-number |access-list-name> is the name or access-list number to be applied. ***<prefix-list-name>*** is the name of the prefix-list to be applied.

<ifname> specifies the name of interface to be applied with route filtering.

Default:

The function in default situation is disabled.

Command Mode:

Router mode and address-family mode

Usage Guide:

The filter will be applied to all the interfaces in case no specific interface is set.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix myfilter in vlan 1

31.11 exit-address-family

Command:

exit-address-family

Function:

Exit address-family mode

Command Mode:

address-family mode

Example:

Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf IPI
Switch(config-router-af)# exit-address-family
Switch(config-router)#

31.12 ip rip aggregate-address

Command:

ip rip aggregate-address A.B.C.D/M

no ip rip aggregate-address A.B.C.D/M

Function:

To configure RIP aggregation route. The no form of this command will delete this configuration.

Parameter:

A.B.C.D/M:IPv4 address and mask length.

Command Mode:

Router Mode or Interface Configuration Mode.

Default:

Disabled.

Usage Guide:

If to configure aggregation route under router mode, RIP protocol must be enabled. If configured under interface configuration mode, RIP protocol may not be enabled, but the aggregation router can operation after the RIP protocol be enabled on interface.

Example:

To configure aggregation route as 192.168.20.0/22 globally.

```
Switch(config)#router rip
```

```
Switch(config-router) #ip rip agg 192.168.20.0/22
```

31.13 ip rip authentication key-chain

Command:

ip rip authentication key <*name-of-chain*>

no ip rip authentication key-chain

Function:

Use this command to enable RIPV2 authentication on an interface and further configures the adopted key chain. The "**no ip rip authentication key-chain**" command cancels the authentication.

Parameter:

<name-of-chain> is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes.

Default:

Not configured.

Command Mode:

Interface Configuration Mode.

Usage Guide:

If the authentication is only configured without configuring the key chain or password used by the interface, the authentication does no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The "no ip rip authentication key" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.

Example:

```
Switch# config terminal
```

```
Switch(config)# interface vlan 1
```

```
Switch(Config-if-Vlan1)# ip rip authentication key my key
```

Relevant Commands:

key, key chain

31.14 ip rip authentication mode

Command:

ip rip authentication mode {text|md5}

no ip rip authentication mode {ext|md5}

Function:

Configure the authentication mode; the "**no ip rip authentication mode {ext|md5}**" command restores to the default authentication mode namely text authentication mode.

Parameter:

text means text authentication; **md5** means MD5 authentication.

Default:

Not configured authentication.

Command Mode:

Interface Configuration Mode.

Usage Guide:

RIP-I do not support authentication which the RIP-II supports two authentication modes: text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication mode md5
```

Related Command:

ip rip authentication key-chain, ip rip authentication string

31.15 ip rip authentication string

Command:

ip rip authentication string <*text*>

no ip rip authentication string

Function:

Set the password used in RIP authentication. The "**no ip rip authentication string**" cancels the authentication.

Parameter:

<text> is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter.

Command Mode:

Interface mode

Usage Guide:

The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The "**no ip rip authentication string**" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication string guest
```

Related Command:

ip rip authentication mode

31.16 ip rip authentication cisco-compatible

Command:

ip rip authentication cisco-compatible

no ip rip authentication cisco-compatible

Function:

After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication.

Parameter:

None

Default:

Not configured

Command Mode:

Interface mode

Usage Guide:

After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.

Example:

```
Switch# config terminal
```

Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication cisco-compatible

Related Command:

ip rip authentication mode

31.17 ip rip receive-packet

Command:

ip rip receive-packet

no ip rip receive-packet

Function:

Set the interface to be able to receivable RIP packets; the "**no ip rip receive-packet**" command set the interface to be unable to receivable RIP packets.

Default:

Interface receives RIP packets.

Command Mode:

Interface Configuration Mode.

Example:

Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip receive-packet

Related Command:

ip rip send-packet

31.18 ip rip receive version

Command:

ip rip receive version { 1 | 2|1 2 }

no ip rip receive version

Function:

Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip receive version**" command restores the value set by using the version command.

Parameter:

1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default:

Version 2

Command Mode:

Interface Configuration Mode.

Example:

Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip receive version 1 2

Related Command:

Version

31.19 ip rip send-packet

Command:

ip rip send-packet

no ip rip send-packet

Function:

Set the Interface to be able to receive the RIP packets; the "**no ip rip send-packet**" set the interface to be unable to receive the RIP packets.

Default:

Interface sends RIP packets.

Command Mode:

Interface Configuration Mode.

Example:

Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip send-packet

Related Command:

ip rip receive-packet

31.20 ip rip send version

Command:

ip rip send version { 1 | 2 | 1-compatible | 1 2}

no ip rip send version

Function:

Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip send version**" command restores the value set by using the version command.

Parameter:

1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default:

Version 2

Command Mode:

Interface Configuration Mode.

Example:

Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip send version 1

Related Command:

Version

31.21 ip rip split-horizon

Command:

ip rip split-horizon [poisoned]

no ip rip split-horizon

Function:

Enable split horizon. The "**no ip rip split-horizon**" disables the split horizon.

Parameter:

[poisoned] means configure the split horizon with poison reverse.

Default:

Split Horizon with poison reverse by default.

Command Mode:

Interface Configuration Mode.

Usage Guide:

The split horizon is for preventing the Routing Loops, namely preventing the layer 3 switches from broadcasting the routes which is learnt from the same interface on which the route to be broadcasted.

Example:

Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip split-horizon poisoned

31.22 key

Command:

key <*keyid*>

no key <*keyid*>

Function:

This command is for managing and adding keys in the key chain. The "**no key <*keyid*>**"command deletes one key.

Parameter:

<keyid> is key ID, ranging between 0-2147483647.

Command Mode:

Keychain mode and keychain-key mode

Usage Guide:

The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example:

Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)#

Relevant Commands:

key chain, key-string, accept-lifetime, send-lifetime

31.23 key chain

Command:

key chain <*name-of-chain*>

no key chain < *name-of-chain* >

Function:

This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < *name-of-chain* >**"deletes one keychain.

Parameter:

<name-of-chain> is the name string of the keychain the length of which is not specifically limited.

Command Mode:

Global Mode

Example:

Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)#

Relevant Commands:

key, key-string, accept-lifetime, send-lifetime

31.24 key-string

Command:

key-string <*text*>

no key-string <*text*>

Function:

Configure a password corresponding to a key. The "**no key-string <*text*>**"command delete the corresponding password.

Parameter:

<text> is a character string without length limit. However when referred by RIP authentication only the first 16 characters will be used.

Command Mode:

Keychain-key mode

Usage Guide:

This command is for configure different passwords for keys with different ID.

Example:

Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string prime

Related Command:

key, key chain, accept-lifetime, send-lifetime

31.25 maximum-prefix

Command:

maximum-prefix <*maximum-prefix*> [<*threshold*>]

no maximum-prefix

Function:

Configure the maximum number of RIP routes in the route table. The "**no maximum-prefix**" command cancels the limit.

Parameter:

<maximum-prefix> the maximum number of RIP route, ranging between 1-65535; a warning is given when the number rate of current route exceeds ***<threshold>*** ranging between 1-100, default at 75.

Command Mode:

router mode

Usage Guide:

The maximum RIP route only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison

is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# maximum-prefix 150

31.26 neighbor

Command:

neighbor <*A.B.C.D*>

no neighbor <*A.B.C.D*>

Function:

Specify the destination address requires targeted-peer sending. The "**no neighbor <*A.B.C.D*>**"command cancels the specified address and restores all gateways to trustable.

Parameter:

<*A.B.C.D*> is the specified destination address for the sending, shown in dotted decimal notation.

Default:

Not sending to any targeted-peer destination address.

Command Mode:

Router mode

Usage Guide:

When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# neighbor 1.1.1.1

Related Command:

passive-interface

31.27 network

Command:

network <*A.B.C.C/M*|*ifname*>

no network <*A.B.C.C/M*|*ifname*>

Function:

Configure the RIP protocol network.

Parameter:

<A.B.C.C/M\|> is the IP address prefix and its length in the network.

<ifname> is the name of a interface.

Default:

Not running RIP protocol

Command Mode:

Router mode and address-family mode

Usage Guide:

Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0/8
Switch(config-router)# network vlan 1

Related Command:

show ip rip, clear ip rip

31.28 offset-list

Command:

offset-list <*access-list-number* \|*access-list-name*> {in\|out} <*number* > [<*ifname*>]

no offset-list <*access-list-number* \|*access-list-name*> {in\|out} <*number* > [<*ifname*>]

Function:

Add an offset value to the metric value of the routes learnt by RIP. The "**no offset-list <*access-list-number* \|*access-list-name*> {in\|out} <*number* > [<*ifname*>]**" command disables this function.

Parameter:

< *access-list-number* \|*access-list-name*> is the access-list or name to be applied. ***<number >*** is the added offset value, ranging between 0-16; ***<ifname>*** is the specific interface name

Default:

Default offset value is the metric value defined by the system.

Command Mode:

Router mode and address-family mode

Example:

Switch# config terminal
Switch(config)# router rip

```
Switch(config-router)# offset-list 1 in 5 vlan 1
```

Related Command:

access-list

31.29 passive-interface

Command:

passive-interface *<ifname>*

no passive-interface *<ifname>*

Function:

Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor.

Parameter:

<ifname> is the name of specific interface.

Default:

Not configured

Command Mode:

Router mode

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# passive-interface vlan 1
```

Related Command:

show ip rip

31.30 recv-buffer-size

Command:

recv-buffer-size<*size*>

no recv-buffer-size

Function:

This command configures the size of UDP receiving buffer zone of RIP; the "**no recv-buffer-size**" command restores the system default.

Parameter:

<size> is the buffer zone size in bytes, ranging between 8192-2147483647.

Default:

8192 bytes.

Command Mode:

Router mode

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# recv-buffer-size 23456789

31.31 redistribute

Command:

redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<*value*>] [route-map<*word*>]

no redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<*value*>] [route-map<*word*>]

Function:

Introduce the routes learnt from other routing protocols into RIP.

Parameter:

kernel introduce from kernel routes;

connected introduce from direct routes;

static introduce from static routes;

ospf introduce from OSPF routes. process-id is OSPF process ID, if there is no parameter that means the process by default, range between 1 to 65535;

isis introduce from ISIS routes;

bgp introduce from BGP routes;

<value> is the metric value assigned to the introduced route, ranging between 0 to 16;

<word> is the probe pointing to the route map for introducing routes.

Command Mode:

Router Mode and address-family Mode

Usage Guide:

Under the address-family mode, the parameter kernel and ISIS is unavailable.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# redistribute kernel route-map ipi

To redistribute OSPFv2 routing information to RIP.

Switch(config)# router rip
Switch(config-router)# redistribute ospf 2

31.32 route

Command:

route *<A.B.C.D/M>*

no route *<A.B.C.D/M>*

Function:

This command configures a static RIP route. The "**no route *<A.B.C.D/M>***"command deletes this route.

Parameter:

Specifies this destination IP address prefix and its length.

Command Mode:

Router mode

Usage Guide:

The command add a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.

Example:

Switch# config terminal
Switch(config)# router rip
Switch(config-router)# route 1.0.0.0/8

31.33 router rip

Command:

router rip

no router rip

Function:

Enable the RIP routing process and enter the RIP mode; the "**no router rip**" command closes the RIP routing protocol.

Default:

Not running RIP route.

Command Mode:

Global mode

Usage Guide:

This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.

Example:

Enable the RIP protocol mode

Switch(config)#router rip
Switch(config-router)#

31.34 send-lifetime

Command:

send-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no send-lifetime

Function:

Use this command to specify a key on the keychain as the time period of sending keys. The "**no send-lifetime**" cancels this configuration.

Parameter:

<start-time> parameter specifies the starting time of the time period, which is:

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 - 2035

end-time> Specifies the due of the time period, of which the form should be:

end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

<month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 -2035

<seconds> is the valid period of the key in seconding and ranging between 1-2147483646

Default:

No default configuration

Command Mode:

Keychain-key mode

Usage Guide:

Refer to the 3.13 RIP authentication section.

Example:

The example below shows the send-lifetime configuration on the keychain named mychain for key 1.

Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

Related Command:

key, key-string, key chain, accept-lifetime

31.35 show debugging rip

Command:

show debugging rip

Function:

Show RIP event debugging, RIP packet debugging and RIP nsm debugging status.

Command Mode:

Admin and configuration mode

Example:

```
Switch# show debugging rip
```

RIP debugging status:

RIP event debugging is on

RIP packet detail debugging is on

RIP NSM debugging is on

31.36 show ip protocols rip

Command:

show ip protocols rip

Function:

Show the RIP process parameter and statistics information.

Command Mode:

Admin and configuration mode

Example:

show ip protocols rip

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 8 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 1

Redistributing: static

```
Default version control: send version 2, receive version 2
    Interface            Send   Recv    Key-chain
    Vlan1      2        2

Routing for Networks:
    Vlan1
    Vlan2

Routing Information Sources:
    Gateway          Distance    Last Update   Bad Packets   Bad Routes
    20.1.1.1              120    00:00:31             0             0
```

Distance: (default is 120)

Displayed information Explanation
Sending updates every 30 seconds with +/-50%, next due in 8 seconds Sending update every 30 secs
Timeout after 180 seconds, garbage collect after 120 seconds The route time-out event period is 180 secs, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set Incoming update filter list for all interface is not set
Default redistribution metric is 1 Default redistribution metric is 1
Redistributing: static Redistributing the static route into the RIP route
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet0/0/8 2 2 The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Routing for Networks: Vlan1 Vlan2 The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update Bad Packets Bad Routes 20.1.1.1 120 00:00:31 0 0 Routing information sources The badpacketand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120
Distance: (default is 120) Default manage distance is 120

31.37 show ip rip

Command:

show ip rip

Function:

Show the routes in the RIP route data base.

Command Mode:

Admin mode

Example:

show ip rip

```
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B - BGP
```

	Network	Next Hop	Metric	From	If	Time
R	12.1.1.0/24	20.1.1.1	2	20.1.1.1	Vlan1	02:51
R	20.1.1.0/24		1		Vlan1	

Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/8 with a metric value of 2, and still has 2 minutes 51 seconds before time out.

31.38 show ip rip database

Command:

show ip rip database

Function:

Show the routes in the RIP route database.

Command Mode:

Admin mode

Example:

```
Switch# show ip rip database
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B -BGP
```

	Network	Next Hop	Metric	From	If	Time
R	10.1.1.0/24		1		Vlan1	
R	20.1.1.0/24		1		Vlan2	

Command:

show ip rip

31.39 show ip rip interface

Command:

show ip rip interface [<*ifname*>]

Function:

Show the RIP related messages.

Parameter:

<ifname> is the name of the interface to show the messages.

Command Mode:

Admin mode

Example:

```
Switch# show ip rip interface vlan 1
Vlan1 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:10.1.1.1/24
```

31.40 show ip rip aggregate

Command:

show ip rip aggregate

Function:

To display the information of IPv4 aggregation route.

Parameter:

None.

Command Mode:

Admin and Configuration Mode.

Default:

None.

Usage Guide:

This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on. If configured under global mode, then the interface display “----”, “Metric” is metric. “Count” is the number of learned aggregation routes. “Suppress” is the times of aggregation.

Example:

To display the information of IPv4 aggregation route.

```
Switch(Config-if-Vlan1)#show ip rip agg
```

```
Aggregate information of rip

    Network          Aggregated Ifname    Metric Count Suppress
    192.168.0.0/16     Vlan1                1      2      0
    192.168.4.0/22       ----               1      2      0
    192.168.4.0/24       ----               1      1      1
                       Vlan1                1      1      1
```

Displayed information Explaination
Network Route prefix and prefix length.
Aggregated Ifname To configure the interface name of the aggregation route. If the route aggregated globally, then display “----”.
Metric Metric of aggregation route.
Count The number of learned aggregation route.
Suppress The times of aggregated for aggregation route.

31.41 timers basic

Command:

timers basic *<update> <invalid> <garbage>*

no timers basic

Function:

Adjust the RIP timer update, timeout, and garbage collecting time. The “**no timers basic**” command restores each parameters to their default values.

Parameter:

<update> time interval of sending update packet, shown in seconds and ranging between 5-2147483647;

<invalid> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647;

<garbage> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.

Default:

<update> defaulted at 30;

<invalid> defaulted at 180;

<garbage> defaulted at120

Command Mode:

Router mode

Usage Guide:

The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.

Example:

Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds.

```
Switch(Config-Router)#timers basic 20 80 60
```

31.42 version

Command:

version {1| 2}

no version

Function:

Configure the version of all RIP data packets sent/received by router interfaces: the "**no version**" restores the default configuration.

Parameter:

1 is version 1 rip;

2 is version 2 rip.

Default:

Sent and received data packet is version 2 by default.

Command Mode:

Router mode and address-family mode

Usage Guide:

1. refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets.

2. refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.

Example:

Configure the version of all RIP data packets sent/received by router interfaces to version 2.

```
Switch(config-router)#version 2
```

Related Command:

ip rip receive version

ip rip send version

Chapter 32 Commands for RIPng

32.1 clear ipv6 route

Command:

clear ipv6 rip route {*<ipv6-address >*| kernel |static | connected |rip |ospf |isis | bgp |all }

Function:

Clear specific route from the RIPng route table.

Parameter:

Clears the route exactly match with the destination address from the RIP route table.

<ipv6-address > is the destination address shown in hex notation with prefix length.

kernel delete kernel route from the RIPng route table

static delete static route from the RIPng route table

connected delete direct route from the RIPng route table

rip delete RIPng route from the RIPng route table only

ospf delete IPv6 OSPF route from the RIPng route table only

bgp delete IPv6 BGP route from the RIPng route table only

ISIS delete ivp6 isis route from the RIPng route table only

all delete all routes from the RIPng route table

Default:

No default configuration

Command Mode:

Admin mode

Usage Guide:

All routes in the RIPng route table will be deleted by using this command with all parameters.

Example:

Switch#clear ipv6 rip route 2001:1:1::/64
Switch#clear ipv6 rip route ospf

32.2 default-information originate

Command:

default-information originate

no default-information originate

Function:

Permit redistributing the network 0:: into RIPng. The "**no default-information originate**" disables this function.

Parameter:

None

Default:

Disabled

Command Mode:

Router mode

Example:

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#default-information originate
```

32.3 default-metric

Command:

default-metric <*value*>

no default-metric

Function:

Set the default metric route value of the introduced route; the "**no default-metric**" restores the default value.

Parameter:

<value> is the route metric value to be set, ranging between 1～16.

Default:

Default route metric value is 1.

Command Mode:

Router mode

Usage Guide:

default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIPng routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example:

Set the default route metric value of the routes from other routing protocols when distributed into the RIPng routes as 3.

```
Switch(config-router)#default-metric 3
```

Related Command:

Redistribute

32.4 distance

Command:

distance <*number*> [<*ipv6-address*>] [<*access-list-name* | *access-list-number*>]

no distance [<*ipv6-address*>]

Function:

Set the managing distance with this command. The "**no distance [<*A.B.C.D/M*>]"** command restores the default value to 120.

Parameter:

<number> specifies the distance value, ranging between 1-255.

<ipv6-address> is the local link address or its prefix.

<access-list-name|access-list-number> specifies the access-list number or name applied.

Default:

The default managing distance of RIP is 120.

Command Mode:

Router mode and address-family mode.

Usage Guide:

In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is , the more reliable will be the route acquired from the protocol.

Example:

Switch#config terminal
Switch(config)#router rip
Switch(config-router)#distance 8 fe80:1111::4200:21ff:fe00:11 mylist

32.5 distribute-list

Command:

distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]

no distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]

Function:

This command uses access-list or prefix-list to filter the route renews messages sent and received. The "**no distribute-list {*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]**" command cancels this filter function.

Parameter:

<access-list-name> is the name or access-list number to be applied.

<prefix-list-name> is the name of the prefix-list to be applied.

<ifname> specifies the name of interface to be applied with route filtering.

Default:

Function disabled by RIPng by default.

Command Mode:

Router mode

Usage Guide:

The filter will be applied to all interfaces if no specific interface is set.

Example:

Switch#config terminal
Switch(config)#router ipv6 rip

```
Switch(config-router)#distribute-list prefix myfilter in Vlan1
```

32.6 debug ipv6 rip

Command:

debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]

no debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]

Function:

For opening various debugging switches of RIPng, showing various debugging messages. The "**no debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]**" command close the corresponding debugging switch.

Parameter:

events shows the debugging message of RIPng events

nsm shows the communication messages between RIPng and NSM.

packet shows the debugging messages of RIPng data packets

recv shows the messages of the received data packets

send shows the messages of the sent data packets

detail shows the messages of the data packets received or sent.

Default:

Not enabled

Command Mode:

Admin mode

Example:

```
Switch#debug ipv6 rip packet
```

```
Switch#1970/01/01 21:15:08 IMI: SEND[Ethernet1/10]: Send to [ff02::9]:521
1970/01/01 21:15:08 IMI: SEND[Ethernet1/2]: Send to [ff02::9]:521
1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: Receive from [fe80::20b:46ff:fe57:8e60]:521
1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: 3000:1:1::/64 is filtered by access-list dclist
1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: 3ffe:1:1::/64 is filtered by access-list dclist
1970/01/01 21:15:15 IMI: RECV[Ethernet1/2]: Receive from [fe80::203:fff:fe01:257c]:521
```

32.7 debug ipv6 rip redistribute message send

Command:

debug ipv6 rip redistribute message send

no debug ipv6 rip redistribute message send

Function:

To enable the debugging of sending messages for routing redistribution messages from OSPFv3 or other external process for RIPng. The no form of this command will disable the debugging messages.

Parameter:

None.

Default:

Close the debug by default.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

Switch# debug ipv6 rip redistribute message send
Switch# no debug ipv6 rip redistribute message send

32.8 debug ipv6 rip redistribute route receive

Command:

debug ipv6 rip redistribute route receive

no debug ipv6 rip redistribute route receive

Function:

To enable the debugging switch received from NSM for redistribution of routing information for RIPng. The no form of this command will disable the debugging switch.

Parameter:

None.

Default:

Close the debug by default.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

Switch#debug ipv6 rip redistribute route receive
Switch# no debug ipv6 rip redistribute route receive

32.9 ipv6 rip aggregate-address

Command:

ipv6 rip aggregate-address X:X::X:X/M

no ipv6 rip aggregate-address X:X::X:X/M

Function:

To configure IPv6 aggregation route. The no form of this command deletes the IPv6 aggregation route.

Parameter:

X:X::X:X/M: IPv6 address and prefix length.

Command Mode:

Router Mode or Interface Configuration Mode.

Default:

No aggregation route configured.

Usage Guide:

If to configure aggregation route under router mode, RIPng protocol must be enabled. If configured under interface configuration mode, RIPng protocol may not be enabled, but the aggregation route can operation after the RIPng protocol be enabled on interface.

Example:

To configure aggregation route as 2001:3f:ed8::99/64 globally.

Switch(config)#router rip
Switch(config-router) #ipv6 rip agg 2001:3f:ed8::99/64

32.10 ipv6 rip split-horizon

Command:

ipv6 rip split-horizon [poisoned]

no ipv6 rip split-horizon

Function:

Permit the split horizon. The "**no ipv6 rip split-horizon**" disables the split horizon.

Parameter:

[poisoned] configures split horizon with poison reverse.

Default:

Split horizon with poison reverse.

Command Mode:

Interface Configuration Mode.

Usage Guide:

The split horizon is for preventing the routing loops, namely preventing the layer 3 switch from broadcasting a route at the interface from which the very route is learnt. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal
Switch(config)#interface Vlan1
Switch(config-if-Vlan1)#ipv6 rip split-horizon poisoned

32.11 ipv6 router rip

Command:

ipv6 router rip

no ipv6 router rip

Function:

Enable RIPng on the interface. The “no ipv6 router rip” command disables RIPng on the interface.

Default:

Not configured

Command Mode:

Interface Configuration Mode.

Usage Guide:

The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

```
Switch#config terminal
Switch(config)#interface Vlan1
Switch(Config-if-Vlan1)#ipv6 router rip
```

32.12 neighbor

Command:

neighbor <*ipv6-address*> {<*ifname*> vlan <*vlan-id*>}

no neighbor <*ipv6-address*> {<*ifname*> vlan <*vlan-id*>}

Function:

Specify the destination address for fixed sending. The “**no neighbor <*ipv6-address*> <*ifname*> vlan <*vlan-id*>** “cancels the specified address defined and restores all trusted gateways.

Parameter:

<ipv6-address> is the IPv6 Link-local address specified for sending and shown in colon hex notation without the prefix length. ***<ifname>*** is the name of interface.

Default:

Not sending to any fixed destination address.

Command Mode:

Router mode

Usage Guide:

When used associating passive-interface command it would be able to send routing messages to specified neighbor only.

Example:

```
Switch#config terminal
```

Switch(config)#router ipv6 rip
Switch(config-router)#neighbor FE80:506::2 Vlan1

Related Command:

passive-interface

32.13 offset-list

Command:

offset-list <*access-list-number*|*access-list-name*> {in|out} <*number* >[<*ifname*>|vlan <*vlan-id*>]

no offset-list <*access-list-number*|*access-list-name*> {in|out }<*number* >[<*ifname*>|vlan <*vlan-id*>]

Function:

Add an offset value on the routing metric value learnt by RIPng. The "**no offset-list <*access-list-number*|*access-list-name*> {in|out}<*number* >[<*ifname*>|vlan <*vlan-id*>]**" command disables this function.

Parameter:

<access-list-number |access-list-name> is the access-list or name to be applied.

<number> is the additional offset value, ranging between 0-16;

<ifname> is the name of specific interface.

Default:

The default offset value is the metric value of the interface defined by the system.

Command Mode:

Router mode

Example:

Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#offset-list 1 in 5 Vlan1

Related Command:

access-list

32.14 passive-interface

Command:

passive-interface<*ifname*>|vlan <*vlan-id*>

no passive-interface<*ifname*>|vlan <*vlan-id*>

Function:

Set the RIPng layers 3 switches to block RIPng broadcast on the specified interfaces, and only send the RIPng data packet to the layer 3 switch which is configured with neighbor.

Parameter:

<ifname> is the specific interface name.

Default:

Not configured

Command Mode:

Router mode

Example:

Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#passive-interface Vlan1

Related Command:

show ipv6 rip

32.15 redistribute

Command:

redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

Function:

Introduce the routes learnt from other routing protocols into RIPng.

Parameter:

kernel introduce from kernel routes

connected introduce from direct routes

static introduce from static routes

ospf introduce from IPv6 OSPF routes

isis introduce from IPv6 ISIS routes

bgp introduce from IPv6 BGP routes

<value> is the metric value assigned to the introduced route, ranging between 0-16

<word> is the probe poining to the route map for introducing routes

Command Mode:

Router mode

Example:

Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#redistribute kernel route-map ip

32.16 redistribute ospf

Command:

redistribute ospf [<*process-tag*>] [metric<*value*>] [route-map<*word*>]

no redistribute ospf [<*process-tag*>]

Function:

To redistribute routing information from external OSPFv3 processes to RIPng process. The no form of this command will remove the introduced OSPFv3 routing entries.

Parameters:

process-tag is the string tag for OSPFv3 process with maximum length limited within 15 characters. If not specified, the default process will be used.

metric<*value*> is the metric for the introduced routing entries, limited between 0 and 16.

route-map<*word*> is the pointer to the introduced routing map.

Default:

Not redistributed by default.

Command Mode:

RIPng Configuration Mode.

Usage Guide:

None.

Example:

To redistribute OSPFv3 ABC routing ro RIPng.

```
Switch(config)#router ipv6 rip
Switch (config-router)#redistribute ospf abc
```

32.17 route

Command:

route <*ipv6-address*>

no route <*ipv6-address*>

Function:

This command configures a static RIPng route. The "**no route <*ipv6-address*>**" command deletes this route.

Parameter:

Specifies this destination IPv6 address prefix and its length show in colon hex notation.

Usage Guide:

The command adds a static RIPng route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIPng route database, however it could be located by using the show ipv6 rip command.

Command Mode:

Router mode

Example:

```
Switch#config terminal
```

```
Switch(config)#router ipv6 rip
Switch(config-router)#route 3ffe:1234:5678::1/64
```

32.18 router ipv6 rip

Command:

router ipv6 rip

no router ipv6 rip

Function:

Enable RIPng routing process and entering RIPng mode; the "**no router ipv6 rip**" of this command disables the RIPng routing protocol.

Default:

RIPng routing not running.

Command Mode:

Global mode

Usage Guide:

This command is for enabling the RIPng routing protocol, this command should be enabled before performing other global configuration of the RIPng protocol.

Example:

Enable the RIPng protocol mode.

```
Switch(config)#router ipv6 rip
```

32.19 show debugging ipv6 rip

Command:

show debugging ipv6 rip

Function:

Show RIPng debugging status for following debugging options: nsm debugging, RIPng event debugging, RIPng packet debugging and RIPng nsm debugging.

Command Mode:

Admin mode

Example:

```
Switch#show debugging ipv6 rip
RIPng debugging status:
  RIPng event debugging is on
  RIPng packet detail debugging is on
RIPng NSM debugging is on
```

32.20 show ipv6 rip interface

Command:

show ipv6 rip interface

Function:

Make sure the interface and line protocols is up.

Command Mode:

Admin mode

Example:

```
Switch(config)#show ipv6 rip interface
Loopback is up, line protocol is up
  RIPng is not enabled on this interface
Vlan1 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      3000:1:1::1/64
      fe80::203:fff:fe0c:cda/64
```

Displayed information Explanations
Vlan1 is up, line protocol is up Interface is Up
Routing Protocol: RIP The routing protocol running on the interface is RIPng
Passive interface: Disabled Passive-interface disabled
Split horizon: Enabled with Poisoned Reversed The split horizon is enabled with poisoned reversed on the interface.
IP interface address: 3000:1:1::1/64 fe80::203:fff:fe01:429e/64 IPv6 address of the interface

32.21 show ipv6 rip redistribute

Command:

show ipv6 rip redistribute

Function:

Show the configuration information of redistributed other out routing to RIPng.

Parameter:

None.

Default:

Not shown by default.

Command Mode:

Admin Mode and Configuration Mode.

Usage Guide:

None.

Example:

```
Switch#show ipv6 rip redistribute
```

32.22 show ipv6 protocols rip

Command:

show ipv6 protocols rip

Function:

Show the RIPng process parameters and statistic messages.

Command Mode:

Admin mode

Example:

```
Switch(config)#show ipv6 protocols rip
  Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-50%, next due in 1 second
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
    Ethernet1/10 filtered by dclist
  Default redistribute metric is 1
  Redistributing: static
  Interface
    Vlan10
    Vlan2
```

Routing for Networks:

Displayed information
Explanations

Sending updates every 30 seconds with +/-50%, next due in 1 seconds Sending updates every 30 seconds
Timeout after 180 seconds, garbage collect after 120 seconds The route timeout time is 180 seconds, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set Incoming update filter list for all interface is not set
Default redistribution metric is 1 Default redistribution metric is 1
Redistributing: static Redistricting the static route into the RIP routes
Interface Vlan10 Vlan2 The interfaces running RIP is Vlan 10 and Vlan 2

32.23 show ipv6 rip

Command:

show ipv6 rip

Function:

Show RIPng Routing.

Command Mode:

Admin mode

Example:

```
Switch#show ipv6 rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B - BGP, a - aggregate, s - suppressed

   Network                    Next Hop                 If        Met Tag  Time
R  2000:1:1::/64              ::                       Vlan2     1   0
R  2001:1:1::/64              fe80::203:fff:fe01:257c  Vlan2     2   0 02:40
R  3000:1:1::/64              ::                       Vlan10    1   0
R  3010:1:1::/64              ::                       --        1   0
```

Amongst R stands for RIP route, namely a RIP route with the destination network address 2001:1:1::/64, next-hop address at fe80::203:fff:fe01:257c. It is learnt from the Ethernet port VLAN2 with a metric value of 2, and still has 2 minutes 40 seconds before time out.

Equal Command:

show ipv6 rip database

32.24 show ipv6 rip database

Command:

show ipv6 rip database

Function:

Show messages related to RIPng database.

Command Mode:

Admin mode

Example:

```
Switch#show ipv6 rip database
```

Equal Command:

show ipv6 rip

32.25 show ipv6 rip aggregate

Command:

show ipv6 rip aggregate

Function:

To display the information of IPv6 aggregation route.

Parameter:

None.

Command Mode:

Admin and Configuration Mode.

Default:

None.

Usage Guide:

This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on, if configured under global mode, then the interface display "----". "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.

Example:

To display the information of IPv6 aggregation route.

```
Switch(config-router)#show ipv rip agg

 Aggregate information of ripng

      Network                 Aggregated Ifname      Metric Count Suppress
      2001::/16               Vlan1                   1      2      0
      2001:1::/32              ----                   1      2      0
      2001:1:2::/60           Vlan1                   1      1      1
                               ----                   1      1      1
```

Displayed information Explaination
Network Route prefix and prefix length.
Aggregated Ifname To configure the interface name of the aggregation route. If the route aggregated globally, then display “---”.
Metric Metric of aggregation route.
Count The number of learned aggregation routes.
Suppress The times of aggregated for aggregation route.

32.26 show ipv6 rip redistribute

Command:

show ipv6 rip redistribute

Function:

Show the configuration information of redistributed other out routing to RIPng.

Parameter:

None.

Default:

Not shown by default.

Command Mode:

Admin Mode and Configuration Mode.

Usage Guide:

None.

Example:

```
Switch#show ipv6 rip redistribute
```

32.27 timers basic

Command:

timers basic <*update*> <*invalid*> <*garbage*>

no timers basic

Function:

Adjust the RIP timer update, timeout, and garbage collecting time. The "**no timers basic**" command restores each parameters to their default values.

Parameter:

<update> time interval of sending update packet, shown in seconds and ranging between 5-2147483647;

<invalid> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647;

<garbage> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.

Default:

<update> defaulted at 30;

<invalid> defaulted at 180;

<garbage> defaulted at120

Command Mode:

Router mode

Usage Guide:

The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.

Example:

Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds.

```
Switch(Config-Router)#timers basic 20 80 60
```

Chapter 33 Commands for OSPF

33.1 area authentication

Command:

area <*id*> authentication [message-digest]

no area <*id*> authentication

Function:

Configure the authentication mode of the OSPF area; the "**no area <*id*> authentication**" command restores the default value.

Parameter:

<id> is the area number which could be shown in digit, ranging between 0 to 4294967295, or in IP address. **message-digest** is proved by MD5 authentication, or be proved by simple plaintext authentication if not choose this parameter.

Default:

No authentication.

Command Mode:

OSPF protocol mode

Usage Guide:

Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use ip ospf authentication-key to set the password while no authentication mode configured at the interface and the area is plaintext authentication, and use ip ospf message-digest key command to configure MD5 key if is MD5 authentication. The area authentication mode could not affect the authentication mode of the interface in this area.

Example:

Set the authentication mode in area 0 to MD5.

```
Switch(config-router)#area 0 authentication message-digest
```

33.2 area default-cost

Command:

area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function:

Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter:

<id> is the area number which could be shown as digits 0～4294967295, or as an IP address; ***<cost>*** ranges between <0-16777215>.

Default:

Default OSPF cost is 1.

Command Mode:

OSPF protocol mode

Usage Guide:

The command is only adaptive to the ABR router connected to the stub area or NSSA area.

Example:

Set the default-cost of area 1 to 10.

```
Switch(config-router)#area 1 default-cost 10
```

33.3 area filter-list

Command:

area <*id*> filter-list {access|prefix} {in|out}

no area <*id*> filter-list {access|prefix} {in|out}

Function:

Configure the filter broadcasting summary routing on the ABR; the "**no area <*id*> filter-list {access|prefix} {in|out}**" command restores the default value.

Parameter:

<id> is the area number which could be shown in digits ranging between 0～4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix;

<name> is the name of the filter, the length of which is between 1-256; in means from other areas to this area, out means from this area to other areas.

Default:

No filter configured.

Command Mode:

OSPF protocol mode

Usage Guide:

This command is used for restraining routes from specific area from spreading between this area and other areas.

Example:

Set a filter on the area 1.

```
Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255
Switch(config)#access-list 1 permit any
Switch(config)#router ospf 100
Switch(config-router)#area 1 filter-list access 1 in
```

33.4 area nssa

Command:

area <*id*> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE | no-summary]

no area <*id*> nssa [TRANSLATOR| no-redistribution | DEFAULT-ORIGINATE | no-summary]

Function:

Set the area to Not-So-Stubby-Area (NSSA) area.

Parameter:

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

TRANLATOR = translator-role {candidate|never|always}, specifies the LSA translation mode for routes: **candidate** means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is **candidate.**

never means the router will never translate Type 7 LSA to Type 5 LSA.

always means the route always translate Type 7 LSA to Type 5 LSA.

no-redistribution means never distribute external-LSA to NSSA.

DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type *<1-2>*], generate the Type-7 LSA.

metric *<0-16777214>* specify the metric value.

metric-type *<1-2>* specifies the metric value type of external-LSA , default value is 2.

no-summary shows not injecting area route to the NSSA.

Default:

No NSSA area defined by default.

Command Mode:

OSPF protocol mode

Usage Guide:

The same area can not be both NSSA and stub at the same time.

Example:

Set area 3 to NSSA.

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#area 0.0.0.51 nssa
Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution

33.5 area range

Command:

area <*id*> range <*address*> [advertise| not-advertise| substitute]

no area <*id*> range <*address*>

Function:

Aggregate OSPF route on the area border. The "**no area *<id>* range *<address>***"cancels this function.

Parameter:

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<address>=<A.B.C.D/M> specifies the area network prefix and its length.

advertise: Advertise this area, which is the default.

not-advertise : Not advertise this area.

substitute= substitute <*A.B.C.D/M*>: advertise this area as another prefix.

<*A.B.C.D/M*>: Replace the network prefix to be advertised in this area.

Default:

Not set.

Command Mode:

OSPF protocol mode

Usage Guide:

Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example:

```
Switch#config terminal
Switch(config)# router ospf 100
Switch(config-router)# area 1 range 192.16.0.0/24
```

33.6 area stub

Command:

area <*id*> stub [no-summary]

no area <*id*> stub [no-summary]

Function:

Define a area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function.

Parameter:

<*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

no-summary: The area border routes stop sending link summary announcement to the stub area.

Default:

Not defined.

Command Mode:

OSPF protocol mode

Usage Guide:

Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example:

```
Switch # config terminal
```

Switch (config)# router ospf 100
Switch (config-router)# area 1 stub

Related Command:

area default-cost

33.7 area virtual-link

Command:

area <*id*> virtual-link A.B.C.D {AUTHENTICATION |AUTH_KEY | INTERVAL}

no area <*id*> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]

Function:

Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <*id*> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]**" command removes this virtual-link.

Parameter:

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

AUTHENTICATION = authentication [message-digest[message-digest-key <1-255> md5 <LINE>] |null|AUTH_KEY].

authentication : Enable authentication on this virtual link.

message-digest: Authentication with MD-5.

null : Overwrite password or packet summary with null authentication.

AUTH_KEY= authentication-key <*key*>.

<key>: A password consists of less than 8 characters.

INTERVAL= [dead-interval | hello-interval | message-digest-key<1-255>md5<LINE> | retransmit-interval | transmit-delay] <value>.

***<value>*:>:** The delay or interval seconds, ranging between 1~65535.

***<dead-interval>*:** A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

***<hello-interval>*:** The time interval before the router sends a hello group message, default is 10 seconds.

<message-digest-key>: Authentication key with MD-5.

***<retransmit-interval>*:** The time interval before a router retransmitting a group message, default is 5 seconds.

***<transmit-delay>*:** The time delay before a router sending a group messages, default is 1 second.

Default:

None.

Command Mode:

OSPF protocol mode

Usage Guide:

In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

Example:

Switch#config terminal
Switch(config) #router ospf 100

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

Relevant Commands:

area authentication, show ip ospf, show ip ospf virtual-links

33.8 auto-cost reference-bandwidth

Command: auto-cost reference-bandwidth <*bandwith*>

no auto-cost reference-bandwidth

Function:

This command sets the way in which OSPF calculate the default metric value. The "**no auto-cost reference-bandwidth**" command only configures the cost to the interface by types.

Parameter:

<bandwith> reference bandwidth in Mbps, ranging between 1~4294967.

Default:

Default bandwidth is 100Mbps.

Command Mode:

OSPF protocol mode

Usage Guide:

The interface metric value is acquired by divide the interface bandwith with reference bandwidth. This command is mainly for differentiate high bandwidth links. If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#auto-cost reference-bandwidth 50

Relative Command:

ip ospf cost

33.9 compatible rfc1583

Command:

compatible rfc1583

no compatible rfc1583

Function:

This command configures to rfc1583 compatible. The "**no compatible rfc1583**" command close the compatibility.

Default:

Rfc 2328 compatible by default.

Command Mode:

OSPF protocol mode

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#compatible rfc1583
```

33.10 clear ip ospf process

Command:

clear ip ospf [<*process-id*>] process

Function:

Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.

Default:

No default configuration.

Command Mode:

Admin mode

Example:

```
Switch#clear ip ospf process
```

33.11 debug ospf events

Command:

debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

Function:

Open debugging switches showing various OSPF events messages; the "**no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink**]" command closes the debugging switch.

Default:

Closed

Command Mode:

Admin and global mode

Example:

```
Switch#debug ospf events router
```

33.12 debug ospf ifsm

Command:

debug ospf ifsm [status|events|timers]

no debug ospf ifsm [status|events|timers]

Function:

Open debugging switches showing the OSPF interface states; the "**no debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf ifsm events
```

33.13 debug ospf lsa

Command:

debug ospf lsa [generate|flooding|install|maxage|refresh]

no debug ospf lsa [generate|flooding|install|maxage|refresh]

Function:

Open debugging switches showing showing link state announcements; the "**no debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf lsa generate
```

33.14 debug ospf nfsm

Command:

debug ospf nfsm [status|events|timers]

no debug ospf nfsm [status|events|timers]

Function:

Open debugging switches showing OSPF neighbor state machine; the "**no debug ospf nfsm [status|events|timers]**"command closes this debugging switch.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf nfsm events
```

33.15 debug ospf nsm

Command:

debug ospf nsm [interface|redistribute]

no debug ospf nsm [interface|redistribute]

Function:

Open debugging switches showing OSPF NSM, the "**no debug ospf nsm [interface|redistribute]**" command closes this debugging switch.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf nsm interface
```

33.16 debug ospf packet

Command:

debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]

no debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]

Function:

Open debugging switches showing OSPF packet messages; the "**no debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]**" command closes this debugging switch.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf packet hello
```

33.17 debug ospf route

Command:

debug ospf route [ase|ia|install|spf]

no debug ospf route [ase|ia|install|spf]

Function:

Open debugging switches showing OSPF related routes; the "**no debug ospf route [ase|ia|install|spf]**" command closes this debugging switch.

Default:

Closed

Command Mode:

Admin mode and global mode

Example:

```
Switch#debug ospf route spf
```

33.18 debug ospf redistribute message send

Command:

debug ospf redistribute message send

no debug ospf redistribute message send

Function:

To enable debugging of sending command from OSPF process redistributed to other OSPF process routing. The no form of command disables debugging of sending command from OSPF process redistributed to other OSPF process routing.

Parameter:

None.

Default:

Disabled.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

To enable debugging of sending command from OSPF process redistributed to other OSPF process routing.

```
Switch#debug ospf redistribute message send
```

33.19 debug ospf redistribute route receive

Command:

debug ospf redistribute route receive

no debug ospf redistribute route receive

Function:

To enable/disable debugging switch of received routing message from NSM for OSPF process.

Parameter:

None.

Default:

Disabled.

Command Mode:

Admin Mode.

Usage Guide:

None.

Example:

To enable debugging switch of received routing message from NSM for OSPF process.

Switch# debug ospf redistribute route receive

33.20 default-information originate

Command:

default-information originate [always | METRIC | METRICTYPE | ROUTEMAP]

no default-information originate

Function:

This command create a default external route to OSPF route area; the "**no default-information originate**" closes this feature.

Parameter:

always: Whether default route exist in the software or not, the default route is always advertised.

METRIC = metric <*value*>: Set the metric value for creating default route, **<*value*>** ranges between 0~16777214, default metric value is 0.

METRICTYPE = metric-type {1|2} set the OSPF external link type of default route.

1 Set the OSPF external type 1 metric value.

2 Set the OSPF external type 2 metric value.

ROUTEMAP = route-map <*WORD*>.

<WORD> specifies the route map name to be applied.

Default:

Default metric value is 10, default OSPF external link type is 2.

Command Mode:

OSPF protocol mode

Usage Guide:

When introducing route into OSPF route area with this command, the system will behaves like an ASBR.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo

Relevant Commands:

route-map

33.21 default-metric

Command:

default-metric <*value*>

no default-metric

Function:

The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter:

<*value*>, metric value, ranging between 0~16777214.

Default:

Built-in, metric value auto translating.

Command Mode:

OSPF protocol mode

Usage Guide:

When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-metric 100

33.22 distance

Command:

distance {<*value*>|ROUTEPARAMETER}

no distance ospf

Function:

Configure OSPF manage distance base on route type. The "**no distance ospf**" command restores the default value.

Parameter:

<*value*>, OSPF routing manage distance, ranging between 1~235

ROUTEPARAMETER= ospf {ROUTE1|ROUTE2|ROUTE3}.

ROUTE1= external <external-distance>, Configure the distance learnt from other routing area.

<external-distance>distance value, ranging between 1~255.

ROUTE2= inter-area <inter-distance>, configure the distance value from one area to another area.

<inter-distance> manage distance value, ranging between 1~255.

ROUTE3= intra-area <intra-distance> Configure all distance values in one area.

<intra-distance> Manage distance value, ranging between 1~255.

Default:

Default distance value is 110.

Command Mode:

OSPF protocol mode

Usage Guide:

Manage distance shows the reliability of the routing message source. The distance value may range between 1~255. The larger the manage distance value is, the lower is its reliability.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40

33.23 distribute-list

Command:

distribute-list <*access-list-name*> out {kernel |connected| static| rip| isis| bgp}

no distribute-list out {kernel |connected| static| rip| isis| bgp}

Function:

Filter network in the routing update. The "**no distribute-list out {kernel |connected| static| rip| isis| bgp}**" command disables this function.

Parameter:

< *access-list-name*> is the access-list name to be applied.

out: Filter the sent route update.

kernel Kernel route.

connected Direct route.

static Static route.

rip RIP route.

isis ISIS route.

bgp BGP route.

Command Mode:

OSPF protocol mode

Usage Guide:

When distributing route from other routing protocols into the OSPF routing table, we can use this command.

Example:

Example below is the advertisement based on the access-list list 1 of the BGP route.

Switch#config terminal
Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf 100
Switch(config-router)#distribute-list 1 out bgp

Switch(config-router)#redistribute bgp

33.24 host area

Command:

host <*host-address*> area <*area-id*> [cost <*cost*>]

no host <*host-address*> area <*area-id*> [cost <*cost*>]

Function:

Use this command to set a stub host entire belongs to certain area. The "**[no] host <*host-address*> area <*area-id*> [cost <*cost*>]**" command cancels this configuration.

Parameter:

<host-address> is host IP address show in dotted decimal notation.

<area-id> area ID shown in dotted decimal notation or integer ranging between 0~4294967295.

<cost> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0.

Default:

No entire set.

Command Mode:

OSPF protocol mode

Usage Guide:

With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#host 172.16.10.100 area 1
Switch(config-router)#host 172.16.10.101 area 2 cost 10

33.25 ip ospf authentication

Command:

ip ospf [<*ip-address*>] authentication [message-digest|null]

no ip ospf [<*ip-address*>] authentication

Function:

Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the "**no ip ospf [<*ip-address*>] authentication**" command cancels the authentication.

Parameter:

<ip-address> is the interface IP address, shown in dotted decimal notation.

message-digest: Use MD5 authentication.

null: no authentication applied, which resets the password or MD5 authentication applied on the interface.

Default:

Authentication not required in receiving OSPF packets on the interface.

Command Mode:

Interface Configuration Mode.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf authentication message-digest

33.26 ip ospf authentication-key

Command:

ip ospf [<*ip-address*>] authentication-key <LINE>

no ip ospf [<*ip-address*>] authentication

Function:

Specify the authentication key required in sending and receiving OSPF packet on the interface; the "**no ip ospf [<*ip-address*>] authentication**" cancels the authentication key.

Parameter:

<ip-address> is the interface IP address shown in dotted decimal notation;

<LINE> specifies the key required in the plaintext authentication.

Default:

Authentication not required in receiving OSPF packets on the interface.

Command Mode:

Interface Configuration Mode.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf authentication-key password

33.27 ip ospf cost

Command:

ip ospf [<*ip-address*>] cost <*cost*>

no ip ospf [<*ip-address*>] cost

Function:

Specify the cost required in running OSPF protocol on the interface; the "**no ip ospf [<*ip-address*>] cost**" command restores the default value.

Parameter:

<ip-address> is the interface IP address shown in dotted decimal notation.

<cost > is the cost of OSPF protocol ranging between 1~65535.

Default:

Default OSPF cost on the interface is auto-figure out based bandwidth.

Command Mode:

Interface Configuration Mode.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf cost 3

33.28 ip ospf database-filter

Command:

ip ospf [<*ip-address*>] database-filter all out

no ip ospf [<*ip-address*>] database-filter

Function:

The command opens LSA database filter switch on specific interface; the "**no ip ospf [<*ip-address*>] database-filter**" command closes the filter switch.

Parameter:

<ip-address> is the interface IP address shown in dotted decimal notation;

all: All LSAs.

out: Sent LSAs.

Default:

Filter switch Closed.

Command Mode:

Interface Configuration Mode.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf database-filter all out

33.29 ip ospf dead-interval

Command:

ip ospf [<*ip-address*>] dead-interval <*time* >

no ip ospf [<*ip-address*>] dead-interval

Function:

Specify the dead interval for neighboring layer 3 switch; the "**no ip ospf [<*ip-address*>] dead-interval**" command restores the default value.

Parameter:

<ip-address> is the interface IP address shown in dotted decimal notation;

<time > is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~65535.

Default:

The default dead interval is 40 seconds (normally 4 times of the hellow-interval).

Command Mode:

Interface Configuration Mode.

Usage Guide:

If no Hello data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf dead-interval 80

33.30 ip ospf disable all

Command:

ip ospf disable all

no ip ospf disable all

Function:

Stop OSPF group process on the interface.

Command Mode:

Interface Configuration Mode.

Usage Guide:

This command resets the network area command and stops group process on specific interface.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf disable all

33.31 ip ospf hello-interval

Command:

ip ospf [<*ip-address*>] hello-interval <*time*>

no ip ospf [<*ip-address*>] hello-interval

Function:

Specify the hello-interval on the interface; the "**no ip ospf [<*ip-address*>] hello-interval**" restores the default value.

Parameter:

<ip-address> is the interface IP address shown in dotted decimal notation;

<time> is the interval sending HELLO packet, shown in seconds and ranging between 1～65535.

Default:

The hello-interval on the interface is 10 seconds.

Command Mode:

Interface Configuration Mode.

Usage Guide:

HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf hello-interval 20

Relevant Commands:

ip ospf dead-interval

33.32 ip ospf message-digest-key

Command:

ip ospf [<*ip-address*>] message-digest-key <*key_id*> MD5 <*LINE*>

no ip ospf [<*ip-address*>] message-digest-key <*key_id*>

Function:

Specify the key id and value of MD5 authentication on the interface; the "**no ip ospf [<*ip-address*>] message-digest-key <*key_id*>**"restores the default value.

Parameter:

<ip-address> is the interface IP address show in dotted decimal notation;

<key_id> ranges between 1-255;

<LINE> is the OSPF key.

Default:

MD5 key not configured.

Command Mode:

Interface Configuration Mode.

Usage Guide:

MD5 key encrypted authentication is used for ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command or else no adjacent relationship will not be created. The last configuration of this command will overwrite the previous one to prevent the system from communicating with the former key id.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf message-digest-key 2 MD5 yourpassword

33.33 ip ospf mtu

Command:

ip ospf mtu <*mtu*>

no ip ospf mtu

Function:

Specify the mtu value of the interface as the OSPF group structure according; the "**no ip ospf mtu**" command restores the default value.

Parameter:

<*mtu*> is the interface mtu value ranging between 576~65535.

Default:

Use the interface mtu acquired from the kernel.

Command Mode:

Interface Configuration Mode.

Usage Guide:

The interface value configured by this command is only used by OSPF protocol other than updated into kernel.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu 1480

33.34 ip ospf mtu-ignore

Command:

ip ospf <*ip-address*> mtu-ignore

no ip ospf <*ip-address*> mtu-ignore

Function:

Use this command so that the mtu size is not checked when switching DD; the "**no ip ospf**

***<ip-address>* mtu-ignore**" will ensure the mtu size check when performing DD switch.

Parameter:

<ip-address> is the interface IP address show in dotted decimal notation.

Default:

Check mtu size in DD switch.

Command Mode:

Interface Configuration Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu-ignore
```

33.35 ip ospf network

Command:

ip ospf network {broadcast | non-broadcast | point-to-point | point-to-multipoint}

no ip ospf network

Function:

This command configures the OSPF network type of the interface; the "**no ip ospf network**" command restores the default value.

Parameter:

broadcast: Set the OSPF network type to broadcast.

non-broadcast: Set the OSPF network type to NBMA.

point-to-point: Set the OSPF network type to point-to-point.

point-to-multipoint: Set the OSPF network type to point-to-multipoint.

Default:

The default OSPF network type is broadcast.

Command Mode:

Interface Configuration Mode.

Example:

The configuration below set the OSPF network type of the interface vlan 1 to point-to-point.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf network point-to-point
```

33.36 ip ospf priority

Command:

ip ospf [<*ip-address*>] priority <*priority*>

no ip ospf [<*ip-address*>] priority

Function:

Configure the priority when electing “Defined layer 3 switch” at the interface. The “**no ip ospf [<*ip-address*>] priority**” command restores the default value.

Parameter:

<ip-address> is the interface IP address show in dotted decimal notation.

<priority> is the priority of which the valid value ranges between 0～255.

Default:

The default priority when electing DR is 1.

Command Mode:

Interface Configuration Mode.

Usage Guide:

When two layer 3 switches connected to the same segments both want to be the “Defined layer 3 switch”, the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as “Defined layer 3 switch” or “Backup Defined layer 3 switch”.

Example:

Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf priority 0

33.37 ip ospf retransmit-interval

Command:

ip ospf [<*ip-address*>] retransmit-interval <*time*>

no ip ospf [<*ip-address*>] retransmit-interval

Function:

Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “**no ip ospf [<*ip-address*>] retransmit-interval**” command restores the default value.

Parameter:

<ip-address> is the interface IP address show in dotted decimal notation.

<time> is the retransmit interveral of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535.

Default:

Default retransmit interval is 5 seconds.

Command Mode:

Interface Configuration Mode.

Usage Guide:

When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.

Example:

Configure the LSA retransmit interval of interface vlan 1 to 10 seconds.

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf retransmit-interval 10

33.38 ip ospf transmit-delay

Command:

ip ospf [<*ip-address*>] transmit-delay <*time*>

no ip ospf [<*ip-address*>] transmit-delay

Function:

Set the transmit delay value of LSA transmitting; the "**no ip ospf [<*ip-address*>] transmit-delay**" restores the default value.

Parameter:

<ip-address> is the interface IP address show in dotted decimal notation.

<time> is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535.

Default:

Default transmit delay value of link state announcements is 1 second.

Command Mode:

Interface Configuration Mode.

Usage Guide:

The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the **transit-delay** prior to sending the LSA, the LSA will be sent before aged.

Example:

Set the LSA transmit delay of interface vlan1 to 3 seconds.

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf transmit-delay 3

33.39 key

Command:

key <*keyid*>

no key <*keyid*>

Function:

This command is for managing and adding keys in the key chain. The "**no key <*keyid*>**" command deletes one key.

Parameter:

<*keyid*> is key ID, ranging between 0-2147483647.

Command Mode:

keychain Mode and keychain-key Mode

Usage Guide:

The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example:

Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#key 1
Switch(config-keychain-key)#

33.40 key chain

Command:

key chain <*name-of-chain*>

no key chain < *name-of-chain* >

Function:

This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < *name-of-chain* >**" command deletes one keychain.

Parameter:

<*name-of-chain*> is the name string of the keychain the length of which is not specifically limited.

Command Mode:

Global Mode and Keychain Mode.

Example:

Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#

33.41 log-adjacency-changes detail

Command:

log-adjacency-changes detail

no log-adjacency-changes detail

Function:

Configure to keep a log for OSPF adjacency changes or not.

Parameter:

None.

Default:

Don't l keep a log for OSPF adjacency changes by default.

Command Mode:

OSPF Protocol Configuration Mode

Usage Guide:

When this command is configured, the OSPF adjacency changes information will be recorded into a log.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#log-adjacency-changes detail

33.42 max-concurrent-dd

Command:

max-concurrent-dd <*value*>

no max-concurrent-dd

Function:

This command set the maximum concurrent number of dd in the OSPF process; the "**no max-concurrent-dd**" command restores the default.

Parameter:

<value> ranges between ***<1-65535>***, which is the capacity of processing the concurrent dd data packet.

Default:

Not set, no concurrent dd limit.

Command Mode:

OSPF protocol mode

Usage Guide:

Specify the max concurrent number of dd in the OSPF process.

Example:

Set the max concurrent dd to 20.

Switch#config terminal
Switch(config)#router ospf 100

Switch(config-router)#max-concurrent-dd 20

33.43 neighbor

Command:

neighbor A.B.C.D [<*cost*>| priority <*value*> | poll-interval <*value*>]

no neighbor A.B.C.D [<*cost*>| priority <*value*> | poll-interval <*value*>]

Function:

This command configures the OSPF router connecting NBMA network. The "**no neighbor A.B.C.D [<*cost*>| priority <*value*> | poll-interval <*value*>]**" command removes this configuration.

Parameter:

<*cost*>, OSPF neighbor cost value ranging between 1-65535;

priority <*value*>, neighbor priority defaulted at 0 and ranges between 0-255;

poll-interval <*value*>, 120s by default, which the polling time before neighbor relationship come into shape , ranging between 1-65535.

Default:

No default configuration.

Command Mode:

OSPF protocol mode

Usage Guide:

Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
Switch(config-router)#neighbor 1.2.3.4 cost 15

33.44 network area

Command:

network NETWORKADDRESS area <*area-id*>

no network NETWORKADDRESS area <*area-id*>

Function:

This command enables OSPF routing function one the interface with IP address matched with the network address. The "**no network NETWORKADDRESS area <*area-id*>**"command removes the configuration and stop OSPF on corresponding interface.

Parameter:

NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W, Shown with the network address prefix or the mask. Wildcast mask if shown in mask;

<area-id> is the ip address or area number shown in point divided demical system, if shown in demcial integer, it ranges between 0~4294967295.

Default:

No default.

Command Mode:

OSPF protocol mode

Usage Guide:

When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.

Example:

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#network 10.1.1.0/24 area 1

33.45 ospf abr-type

Command:

ospf abr-type {cisco|ibm|shortcut|standard}

no ospf abr-type

Function:

Use this command to configure a OSPF ABR type. The "**no ospf abr-type**" command restores the default value.

Parameter:

cisco, Realize through cisco ABR;

ibm, Realize through ibm ABR;

shortcut, Specify a shortcut-ABR;

standard, Realize with standard（RFC2328）ABR.

Default:

Cisco by default.

Command Mode:

OSPF protocol mode

Usage Guide:

For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example:

Configure abr as standard.

Switch#config terminal

Switch(config)#router ospf 100
Switch(config-router)#ospf abr-type standard

33.46 ospf router-id

Command:

ospf router-id <*address*>

no ospf router-id

Function:

Specify a router ID for the OSPF process. The "**no ospf router-id**" command cancels the ID number.

Parameter:

<*address*>, IPv4 address format of router-id.

Default:

No default configuration.

Command Mode:

OSPF protocol mode

Usage Guide:

The new router-id takes effect immediately.

Example:

Configure router-id of ospf 100 to 2.3.4.5.

Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#ospf router-id 2.3.4.5

33.47 overflow database

Command:

overflow database <*maxdbsize* > [{hard|soft}]

no overflow database

Function:

This command is for configuring the max LSA number. The "**no overflow database**" command cancels the limit.

Default:

Not configured.

Parameter:

< *maxdbsize* >Max LSA numbers, ranging between 0~4294967294.

soft: Soft limit, warns when border exceeded.

hard: Hard limit, directly close ospf instance when border exceeded.

If there is not soft or hard configured, the configuration is taken as hard limit.

Command Mode:

OSPF Protocol Mode.

Example:

Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database 10000 soft

33.48 overflow database external

Command:

overflow database external [<*maxdbsize* > <*maxtime*>]

no overflow database external [<*maxdbsize* > <*maxtime*>]

Function:

The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The "**no overflow database external [<*maxdbsize* > <*maxtime*>]**" restores the default value.

Parameter:

< *maxdbsize* > size of external link database, ranging between 0~4294967294, defaulted at 4294967294.

< *maxtime* > the seconds the router has to wait before exiting the database overflow, ranging between 0~65535.

Command Mode:

OSPF protocol mode

Example:

Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database external 5 3

33.49 passive-interface

Command:

passive-interface<*ifname*>

no passive-interface<*ifname*>

Function:

Configure that the hello group not sent on specific interfaces. The "**no passive-interface<*ifname*>**"command cancels this function.

Parameter:

<ifname> is the specific name of interface.

Default:

Not configured.

Command Mode:

OSPF protocol mode

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlan1
```

33.50 redistribute

Command:

redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]

no redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]

Function:

Introduce route learnt from other routing protocols into OSPF.

Parameter:

kernel introduce from kernel route.

connected introduce from direct route.

static introduce from static route.

rip introduce from the RIP route.

isis introduce from ISIS route.

bgp introduce from BGP route.

metric <*value*> is the introduced metric value, ranging between 0-16777214.

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default.

route-map <*word*> point to the probe of the route map for introducing route.

tag<*tag-value*> external identification number of the external route, ranging between 0~4294967295, defaulted at 0.

Command Mode:

OSPF Protocol Mode.

Usage Guide:

Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs.

Example:

```
Switch#config terminal
Switch(config)#router ospf
```

```
Switch(config-router)#redistribute bgp metric 12
```

33.51 redistribute ospf

Command:

redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

no redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function:

To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.

Parameter:

process-id is OSPF process ID, 0 by default.

metric <*value*> is the metric for redistributed routing, range between 0 to 16777214.

metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.

route-map <*word*> is the pointer to the introduced routing map.

Default:

Not redistributed any OSPF routing by default.

Command Mode:

OSPF Protocol Mode.

Usage Guide:

When process-id is not input, that means OSPF routing will be redistributed by default (Process-id is 0).

Example:

```
Switch(config-router)#redistribute ospf
```

33.52 router ospf

Command:

router ospf <process_id>

no router ospf <process_id>

Function:

This command is for relating the OSPF process. The

Example:

```
Switch# config terminal
```

```
Switch(config)# router ospf 100
```

```
Switch(config-router)#network 10.1.1.0/24 area 0
```

33.53 show ip ospf

Command:

show ip ospf [<*process-id*>]

Function:

Display OSPF main messages.

Parameter:

<process-id> is the process ID, ranging between 0~65535.

Default:

Not displayed

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.1.1
 Process bound to VRF default
 Process uptime is 2 days 0 hour 30 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
 Number of areas attached to this router: 1
 Area 0 (BACKBONE) (Inactive)
 Number of interfaces in this area is 0(0)
 Number of fully adjacent neighbors in this area is 0
 Area has message digest authentication
 SPF algorithm executed 0 times
 Number of LSA 0. Checksum Sum 0x000000

 Routing Process "ospf 10" with ID 0.0.0.0
 Process bound to VRF DC1
 Process uptime is 4 days 23 hours 51 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
```

```
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
Area 0 (BACKBONE) (Inactive)
Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has no authentication
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000
```

33.54 show ip ospf border-routers

Command:

show ip ospf [<*process-id*>] border-routers

Function:

Display the intra-domain route entries for the switch to reach ABR and ASBR of all instances.

Parameter:

<process-id> is the process ID, ranging between 0~65535.

Default:

Not displayed

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip ospf border-routers
OSPF process 0 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0
```

33.55 show ip ospf database

Command:

show ip ospf [<*process-id*>] database[{

adv-router [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]

| asbr-summary[{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] | externel [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]

| network [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]

| nssa-external [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] | opaque-area [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]

| opaque-as [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]

|opaque-link [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| router [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]
| summary [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}] |self-originate | max-age }]

Function:

Display the OSPF link state data base messages.

Parameter:

<process-id> is the process ID, ranging between 0~65535

<linkstate_id> Link state ID, shown in point divided demical system

<advertiser_router> is the ID of Advertising router, shown in point divided demcial IP address format

Default:

Not displayed

Command Mode:

Admin and configuration mode

Usage Guide:

According to the output messages of this command, we can view the OSPF link state database messages.

Example:

```
Switch#show ip ospf database
                Router Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum Link count
192.168.1.2     192.168.1.2     254 0x80000031 0xec21 1
192.168.1.3     192.168.1.3     236 0x80000033 0x0521 2

                Net Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum
20.1.1.2        192.168.1.2     254 0x8000002b 0xece4

                Summary Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum   Route
6.1.0.0         192.168.1.2      68 0x8000002b 0x5757  6.1.0.0/22
6.1.1.0         192.168.1.2     879 0x8000002a 0xf8bc  6.1.1.0/24
22.1.1.0        192.168.1.2     308 0x8000000c 0xc8f0  22.1.1.0/24

                ASBR-Summary Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum
192.168.1.1     192.168.1.2    1702 0x8000002a 0x89c7

                AS External Link States
```

```
Link ID         ADV Router      Age Seq#       CkSum  Route
2.2.2.0         192.168.1.1     1499 0x80000056 0x3a63  E2 2.2.2.0/24 [0x0]
2.2.3.0         192.168.1.1     1103 0x8000002b 0x0ec3  E2 2.2.3.0/24 [0x0]
```

33.56 show ip ospf interface

Command:

show ip ospf interface <*interface*>

Function:

Display the OSPF interface messages.

Parameter:

<interface> is the name of interface

Default:

Not displayed

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip ospf interface
Loopback is up, line protocol is up
  OSPF not enabled on this interface
Vlan1 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
    Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
    Transmit Delay is 5 sec, State Waiting, Priority 1
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
      Hello due in 00:00:16
Neighbor Count is 0, Adjacent neighbor count is 0
```

33.57 show ip ospf neighbor

Command:

show ip ospf [<*process-id*>] neighbor [{<*neighbor_id*> |all |detail [all] |interface <*ifaddress*>}]

Function:

Display the OSPF adjacent point messages.

Parameter:

<process-id> is the process ID ranging between 0~65535

<neighbor_id> is the dotted decimal notation neighbor ID

all: Display messages of all neighbors

detail: Display detailed messages of all neighbors

<ifaddress> Interface IP address

Default:

Not displayed

Command Mode:

Admin and configuration mode

Usage Guide:

OSPF neighbor state can be checked by viewing the output of this command.

Example:

```
Switch#show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       1   Full/Backup     00:00:32    6.1.1.1         Vlan1
192.168.1.3       1   Full/DR         00:00:36    20.1.1.3        Vlan2
192.168.1.3       1   Full/ -         00:00:30    20.1.1.3        VLINK2
```

Displayed information Explanation
Neighbor ID ID Neighbor ID
Priority Priority
State Neighbor relation state
Dead time Neighbor dead time
Address Interface Address
Interface Interface name

33.58 show ip ospf redistribute

Command:

show ip ospf [<*process-id*>] redistribute

Function:

To display the routing message redistributed from external process of OSPF.

Parameter:

<process-id> is the process ID ranging between 0~65535.

Default:

None.

Command Mode:

Admin Mode and Configuration Mode.

Usage Guide:

None.

Example:

```
Switch#show ip ospf redistribute
        ospf process 1 redistribute information：
          ospf process 2
          ospf process 3
          bgp
        ospf process 2 redistribute information：
          ospf process 1
          bgp
        ospf process 3 redistribute information：
          ospf process 1
bgp
```

```
Switch#show ip ospf 2 redistribute
        ospf process 2 redistribute information：
          ospf process 1
bgp
```

33.59 show ip ospf route

Command:

show ip ospf [*<process-id>*] route

Function:

Display the OSPF routing table messages.

Parameter: .

<process-id> is the process ID ranging between 0~65535

Default:

Not displayed

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip ospf route


O    10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0
O    10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0
IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
```

```
IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
O   13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3
O   14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4
IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1
E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1
```

33.60 show ip ospf virtual-links

Command:

show ip ospf [<*process-id*>] virtual-links

Function:

Display the OSPF virtual link message.

Parameter:

<process-id> is the process ID ranging between 0~65535.

Default:

Not displayed

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface Vlan1
  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
```

33.61 show ip route process-detail

Command:

show ip route [database] process-detail

Function:

Display the IP routing table with specific process ID or Tag.

Parameters:

The parameter of database means displaying all the routers, no parameter means only displaying effective routers.

Default:

Not importing any router of OSPF process by default.

Command Mode:

Admin mode and configure mode.

Usage Guide:

None.

Example:

```
Switch#show ip route database process-detail
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

C       *> 127.0.0.0/8 is directly connected, Loopback
O           192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13, process 12
C       *> 192.168.2.0/24 is directly connected, Vlan2
```

33.62 show ip protocols

Command:

show ip protocols

Function:

Display the running routing protocol messages.

Default:

None

Command Mode:

Admin and configuration mode

Example:

```
Switch#show ip protocols
Use “show ip protocols” command will show the messages of the routing protocol running on current layer 3 switch
For example, the displayed messages are:
Routing Protocol is "ospf 0"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:
  Routing for Networks:
```

```
    10.1.1.0/24
    12.1.1.0/24
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: (default is 110)
    Address          Mask          Distance List

Routing Protocol is "bgp 0"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
  Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
Incoming Route Filter:
```

33.63 summary-address

Command:

summary-address <*A.B.C.D/M*> [{not-advertise|tag<*tag-value*>}]

Function:

Summarize or restrain external route with specific address scope.

Parameter:

<A.B.C.D/M> address scope, shown in dotted decimal notation IPv4 address plus mask length.

not-advertised restrain the external routes.

tag<*tag-value*> is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0.

Command Mode:

OSPF protocol mode.

Usage Guide:

When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces the size of the link state database.

Example:

```
Switch#config terminal
```

```
Switch(config)#router ospf
```

```
Switch(config-router)#summary-address 172.16.0.0/16 tag 3
```

33.64 timers spf

Command:

timers spf <*spf-delay*> <*spf-holdtime*>

no timers spf

Function:

Adjust the value of the route calculating timer. The "**no timers spf**" command restores relevant values to default.

Parameter:

<*spf-delay*> 5 seconds by default.

<*spf-holdtime*> 10 seconds by default.

Command Mode:

OSPF protocol mode.

Usage Guide:

This command configures the delay time between receiving topology change and SPF calculation, further configured the hold item between two discontinuous SPF calculation.

Example:

Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#timers spf 5 10

Chapter 34 Commands for OSPFv3

34.1 area default cost

Command:

area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function:

Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter:

<*id*> is the area number which could be shown as digits 0～4294967295, or as an IP address; **<*cost*>** ranges between <0-16777215>

Default:

Default OSPFv3 cost is 1.

Command Mode:

OSPFv3 protocol mode

Usage Guide:

The command is only adaptive to the ABR router connected to the stub area.

Example:

Set the default-cost of area 1 to 10

```
Switch(config-router)#area 1 default-cost 10
```

34.2 area range

Command:

area <*id*> range <ipv6*address*> [advertise| not-advertise|]

no area <*id*> range <ipv6*address*>

Function:

Aggregate OSPF route on the area border. The "**no area <*id*> range <*address*>**"cancels this function.

Parameter:

<*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<ipv6*address*>=<*X:X::X:X/M*>,Specifies the area ipv6 network prefix and its length

advertise: Advertise this area

not-advertise : Not advertise this area

If both are not set, this area is defaulted for advertising

Default:

Function not configured.

Command Mode:

OSPFv3 protocol mode

Usage Guide:

Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch (config-router)# area 1 range 2000::/3

34.3 area stub

Command:

area <*id*> stub [no-summary]

no area <*id*> stub [no-summary]

Function:

Define a area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function.

Parameter:

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IPv4 address.

no-summary:

The area border routes stop sending link summary announcement to the stub area

Default:

Not defined

Command Mode:

OSPFv3 protocol mode

Usage Guide:

Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch (config-router)# area 1 stub

Relevant Commands:

area default-cost

34.4 area virtual-link

Command:

area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL <*value*>]

no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL]

Function:

Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area *<id>* virtual-link A.B.C.D [instance-id *<instance-id>* | INTERVAL]**" command removes this virtual-link.

Parameter: <***id***> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<***instance-id***> is the interface instance ID ranging between 0~255 and defaulted at 0

INTERVAL*= [dead-interval*|*hello-interval*|*retransmit-interval*|*transmit-delay***]**

<*value*>: The delay or interval seconds, ranging between 1~65535

***<dead-interval>*:** A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

***<hello-interval>*:** The time interval before the router sends a hello group message, default is 10 seconds

***<retransmit-interval>*:** The time interval before a router retransmitting a group message, default is 5 seconds

***<transmit-delay>*:** The time delay before a router sending a group messages, 1 second by default

Default:

No default configuration.

Command Mode:

OSPFv3 protocol mode

Usage Guide:

In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone areas routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20
Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1

34.5 abr-type

Command:

abr-type {cisco|ibm| standard}

no abr-type [cisco|ibm| standard]

Function:

Configure an OSPF ABR type with this command. The "**no abr-type [cisco|ibm| standard]**" command restores the default.

Parameter: cisco, realize by cisco ABR; **ibm**, realize by ibm ABR; **shortcut**, specify a shortcut-ABR;

standard, realize with standard（RFC2328）ABR.

Default:

Cisco configured by default

Command Mode:

OSPFv3 protocol mode

Usage Guide:

For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example:

Configure ABR as standard.

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#abr-type standard

34.6 default-metric

Command:

default-metric <*value*>

no default-metric

Function:

The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter:

<*value*>, metric value, ranging between 1~16777214.

Default:

Built-in, metric value auto translating.

Command Mode:

OSPF protocol mode

Usage Guide:

When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#default-metric 100

34.7 debug ipv6 ospf events

Command:

[no] debug ipv6 ospf events [abr|asbr|os|router|vlink]

Function:

Open debugging switches showing OSPF events. The "**no debug ipv6 ospf events [abr|asbr|os|router|vlink]**" command closes this debugging switch.

Default:

Closed.

Command Mode:

Admin mode

Example:

```
Switch#debug ipv6 ospf events
1970/01/01 01:10:35 IMI: ROUTER[Process:(null)]: GC timer expire
```

34.8 debug ipv6 ospf ifsm

Command:

[no] debug ipv6 ospf ifsm [status|events|timers]

Function:

Open debugging switches showing the OSPF interface states; the "**[no] debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default:

Closed.

Command Mode:

Admin mode

Example:

```
Switch#debug ipv6 ospf ifsm
1970/01/01 01:11:44 IMI: IFSM[Vlan1]: Hello timer expire
1970/01/01 01:11:44 IMI: IFSM[Vlan2]: Hello timer expire
```

34.9 debug ipv6 ospf lsa

Command:

[no]debug ipv6 ospf lsa [generate|flooding|install|maxage|refresh]

Function:

Open debugging switches showing showing link state announcements; the "**no debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches.

Default:

Closed.

Command Mode:

Admin mode

34.10 debug ipv6 ospf nfsm

Command:

[no] debug ipv6 ospf nfsm [status|events|timers]

Function:

Open debugging switches showing showing OSPF neighbor state machine; the "**no debug ipv6 ospf nfsm [status|events|timers]**"command closes this debugging switch.

Default:

Closed.

Command Mode:

Admin mode

```
Switch#debug ipv6 ospf nfsm
1970/01/01 01:14:07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire
1970/01/01 01:14:07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived)
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)
```

34.11 debug ipv6 ospf nsm

Command: [no] debug ipv6 ospf nsm [interface|redistribute]

Function: Open debugging switches showing showing OSPF NSM, the "**no debug ipv6 ospf nsm [interface|redistribute]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

34.12 debug ipv6 ospf packet

Command: [no] debug ipv6 ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | send]

Function: Open debugging switches showing OSPF packet messages; the "**no debug ipv6 ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | send]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin Mode.

34.13 debug ipv6 ospf redistribute message send

Command: debug ipv6 ospf redistribute message send

no debug ipv6 ospf redistribute message send

Function: To enable/disable debugging of sending command from IPv6 OSPF process redistributed to other IPv6 OSPF process routing.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug ipv6 ospf redistribute message send

34.14 debug ipv6 ospf redistribute route receive

Command: debug ipv6 ospf redistribute route receive

no debug ipv6 ospf redistribute route receive

Function: To enable/disable debugging of received routing message from NSM for IPv6 OSPF process.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug ipv6 ospf redistribute route receive

34.15 debug ipv6 ospf route

Command: [no] debug ipv6 ospf route [ase|ia|install|spf]

Function: Open debugging switches showing OSPF related routes; the "**[no]debug ipv6 ospf route [ase|ia|install|spf]**" command closes this debugging switch.

Default: Closed.

Command Mode: Admin mode

34.16 ipv6 ospf cost

Command: ipv6 ospf cost <*cost*> [instance-id <*id*>]

no ipv6 ospf <*cost*> [instance-id <*id*>]

Function: Specify the cost required in running OSPF protocol on the interface; the "**no ipv6 ospf cost [instance-id <*id*>]**" command restores the default value.

Parameter: ***<id>*** is the interface instance ID, ranging between 0~255, defaulted at 0

<cost > is the cost of OSPF protocol ranging between 1~65535.

Default: Default OSPF cost on the interface is 10.

Command Mode: Interface Configuration Mode.

Usage Guide: The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(Config-if-Vlan1)#ipv6 ospf cost 3

34.17 ipv6 ospf dead-interval

Command: ipv6 ospf dead-interval <*time* > [instance-id <*id*>]

no ipv6 ospf dead-interval [instance-id <*id*>]

Function: Specify the dead interval for neighboring layer 3 switch; the "**no ipv6 ospf dead-interval [instance-id <*id*>]**" command restores the default value.

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*time* > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535

Default: The default dead interval is 40 seconds (normally 4 times of the hello-interval).

Command Mode: Interface Configuration Mode.

Usage Guide: If no HELLO data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

34.18 ipv6 ospf display route single-line

Command: [no] ipv6 ospf display route single-line

Function: show ipv6 ospf route change the display results of show ipv6 ospf route command. The "**no ipv6 ospf display route single-line**" restores to default display mode.

Default: Not configured

Command Mode: Global Mode

Usage Guide: The show ipv6 ospf route command displays the same route in several lines. This command will strict that one route will be displayed in one line.

Example:

Switch # config terminal
Switch(config)#ipv6 ospf display route single-line

34.19 ipv6 ospf hello-interval

Command: ipv6 ospf hello-interval <*time*> [instance-id <*id*>]

no ipv6 ospf hello-interval [instance-id <*id*>]

Function: Specify the hello-interval on the interface; the "**no ipv6 ospf hello-interval [instance-id <*id*>]**" restores the default value.

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*time* > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535

Default: Default HELLO packet sending interval is 10 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch # config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20

Relevant Commands: ipv6 ospf dead-interval

34.20 ipv6 ospf priority

Command: ipv6 ospf priority <*priority*> [instance-id <*id*>]

no ipv6 ospf priority[instance-id <*id*>]

Function: Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ipv6 ospf [<*ip-address*>] priority**" command restores the default value.

Parameter: <*id*> is the interface instance ID, ranging between 0~255, and defaulted at 0

<*priority*> is the priority of which the valid value ranges between 0～255.

Default: The default priority when electing DR is 1.

Command Mode: Interface Configuration Mode.

Usage Guide: When two layer 3 switches connected to the same segments both want to be the "Defined

layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as "Defined layer 3 switch" or "Backup Defined layer 3 switch". The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch # config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf priority 0

34.21 ipv6 ospf retransmit-interval

Command: ipv6 ospf retransmit-interval <*time*> [instance-id <*id*>]

no ipv6 ospf retransmit-interval [instance-id <*id*>]

Function: Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The "**no ipv6 ospf retransmit-interval [instance-id <*id*>]**" command restores the default value.

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*time*> is the retransmit interveral of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535

Default: Default retransmit interval is 5 seconds.

Command Mode: Interface Configuration Mode.

Usage Guide: When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the LSA retransmit interval of interface vlan 1 to 10 seconds.

Switch # config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10

34.22 ipv6 ospf transmit-delay

Command: ipv6 ospf transmit-delay <*time*> [instance-id <*id*>]

no ipv6 ospf transmit-delay [instance-id <*id*>]

Function: Configure the LSA sending delay time on the interface. The "**no ipv6 ospf transmit-delay [instance-id <*id*>]**" command restores to the default.

Parameter: ***<id>*** is the instance ID ranging between 0~255 and defaulted at 0

<time> is the delay time of sending LSA on the interface, which is shown in seconds and ranged between 1～65535.

Default: The default delay time of send LSA on the interface is 1 second by default.

Command Mode: Interface Configuration Mode.

Usage Guide: The LSA ages by time in the layer 3 switches but not in the transmission process. So by increasing the **transmit-delay** before sending LSA so that it will be sent out. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Set the interface vlan 1 LSA sending delay to 3 seconds.

Switch # config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

34.23 ipv6 router ospf

Command: [no] ipv6 router ospf {area <*area-id*> [instance-id <*instance-id*>]| tag <*tag*>[instance-id <*instance-id*>]}| tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}

Function: Enable ospf route on the interface; the "**no ipv6 router ospf {area <*area-id*> [instance-id <*instance-id*>]| tag <*tag*>[instance-id <*instance-id*>]}| tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}**" command cancels this configuration.

Parameter: ***<area-id>*** is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address

<instance-id> is the interface instance ID ranging between 0~255 and defaulted at 0.

<tag> ospfv3 process identifier

Default: Not configured

Command Mode: Interface Configuration Mode.

Usage Guide: To enable this command on the interface, the area id must be configured. The instance ID and instance tag are optional. The ospfv3 process allows one routing instance for each instance ID. The route can be enabled on a interface with a instance ID. If the instance IDs are different, several OSPF process can be run on one interface. However different OSPF process should not use the same instance ID The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch # config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1

34.24 max-concurrent-dd

Command: max-concurrent-dd <*value*>

no max-concurrent-dd

Function: Configure with this command the current dd max concurrent number in the OSPF processing. The "**no max-concurrent-dd**" command restores the default.

Parameter: <*value*> ranges between ***<1-65535>,*** the capacity of concurrent dd data packet processing.

Default: No default configuration. No dd concurrent limit.

Command Mode: OSPFv3 protocol mode

Usage Guide: Specify the current dd max concurrent number in the OSPF processing.

Example: Set the max concurrent dd to 20.

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#max-concurrent-dd 20

34.25 passive-interface

Command: [no] passive-interface {<*ifname*>|vlan <*vlan-id*>}

Function: Configure that the hello group not sent on specific interfaces. The "**no passive-interface{<*ifname*>|vlan <*vlan-id*>}**" command cancels this function.

Parameter: <*ifname*> is the specific name of interface.

Default: Not configured

Command Mode: OSPFv3 protocol mode

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#passive-interface vlan1

34.26 redistribute

Command: [no] redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: Introduce route learnt from other routing protocols into OSPFv3.

Parameter: kernel Introduct from kernel route

connected Introduce from direct route

static Introduce from static route

rip Introduce from the RIP route

isis Introduce from ISIS route

bgp Introduce from BGP route

metric <*value*> is the introduced metric value, ranging between 0-16777214

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default

route-map <*word*> targets to the probe of the route map for introducing route

Command Mode: OSPFv3 protocol mode

Usage Guide: Learn and introduce other routing protocol into OSPFv3 area to generate AS-external_LSAs.

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#redistribute bgp metric 12 metric-type 1

34.27 redistribute ospf

Command: redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type {1|2}] [route-map<*word*>]

no redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: To redistribute routing information form process-tag to this command. The no form of command cancels the redistribution of process-tag routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.

Parameter: process-tag is the process ID of IPv6 OSPF process, NULL by default.

metric <*value*> is the metric for redistributed routing, range between 0 to 16777214.

metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.

route-map <*word*> is the pointer to the introduced routing map.

Default: Not redistributed any OSPFfv3 routing by default.

Command Mode: Router IPv6 OSPF Configuration Mode.

Usage Guide: When process-id is not input, that means OSPFv3 routing will be redistributed by default (Process-tag is NULL). The no form of command input the optional parameters of metric, metric-type and routermap, then restores default configuration. When not input any optional parameters that mean to delete the router of redistributed process.

Example:

Switch (config)# router ipv6 ospf
Switch(config-router)#redistribute ospf

34.28 router-id

Command: router-id <*router-id*>

no router-id

Function: Configure router ID for ospfv3 process. The "**no router-id**"restores ID to 0.0.0.0.

Parameter: <*router-id*>> is the router ID shown in IPv4 format.

Default: 0.0.0.0 by default.

Usage Guide: If the router-id is 0.0.0.0, the ospfv3 process can not be normally enabled. It is required to configure a router-id for ospfv3.

Command Mode: OSPFv3 protocol mode

Example:

Switch # config terminal
Switch (config)# router ipv6 ospf
Switch(config-router)#router-id 192.168.2.1

34.29 router ipv6 ospf

Command: [no] router ipv6 ospf [<*tag*>]

Function: This command initializes the ospfv3 routing prcess and enters ospfv3 mode for configuring the ospfv3 routing process. The "**no router ipv6 ospf [<*tag*>]**" command stops relevant process.

Parameter: <*tag*> ospfv3 is the process mark which could be random strings made up of characters and digits

Command Mode: Global mode

Usage Guide: To let he ospfv3 routing process work properly, this command must be configured and ospfv3 must at least be enabled on one interface. When the tag configured by the ipv6 router ospf area command under interface mode matches with the tag of ospf process, the ospfv3 process is enabled on this interface.

Example:

Switch # config terminal
Switch(config)#router ipv6 ospf IPI

34.30 show ipv6 ospf

Command: show ipv6 ospf [<*tag*>]

Function: Display OSPF global and area messages.

Parameter: <*tag*> is the process tag which is a character string.

Default: Not displayed.

Command Mode: All modes

Example:

```
Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 6
 Number of LSA received 14
 Number of areas in this router is 1
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 6 times
        Number of LSA 8.   Checksum Sum 0x43D52
        Number of Unknown LSA 0
```

34.31 show ipv6 ospf database

Command: show ipv6 ospf [<*tag*>] database

[router [adv-router <*advertiser_router*>]

|network [adv-router <*advertiser_router*>]

| intra-prefix [adv-router <*advertiser_router*>]

| link [adv-router <*advertiser_router*>]

| external [adv-router <*advertiser_router*>]

| inter-prefix [adv-router <*advertiser_router*>]

| inter-router [adv-router <*advertiser_router*>]]

Function: Display the OSPF link state data base message.

Parameter: <*tag*> is the process tag which is a character string.

<*advertiser_router*> is the ID of Advertising router, shown in IPv4 address format

Default: Not displayed

Command Mode: All modes

Usage Guide: According to the output messages of this command, we can view the OSPF link state database messages.

Example:

Use show ipv6 ospf database command will be able to show LSA messages of the OSPF routing protocol For Example, the displayed messages are:

```
OSPFv3 Router with ID (192.168.2.2) (Process *null*)
                    Link-LSA (Interface Vlan1)
Link State ID    ADV Router        Age  Seq#         CkSum  Prefix
0.0.7.211        192.168.2.2       1409 0x80000001 0x6dda      1
0.0.7.212        192.168.2.3       1357 0x80000001 0x248e      1
```

```
                    Link-LSA (Interface Vlan2)
Link State ID    ADV Router      Age  Seq#       CkSum  Prefix
0.0.7.211        192.168.2.1     1450 0x80000001 0xa565     1
0.0.7.212        192.168.2.2     1399 0x80000001 0x4305     1
                    Router-LSA (Area 0.0.0.0)
Link State ID    ADV Router      Age  Seq#       CkSum  Link
0.0.0.0          192.168.2.1     1390 0x80000006 0x9fe2     1
0.0.0.0          192.168.2.2     1354 0x80000007 0x4af5     2
0.0.0.0          192.168.2.3     1308 0x80000004 0xbbc4     1

                    Network-LSA (Area 0.0.0.0)
        Link State ID    ADV Router      Age  Seq#       CkSum
0.0.7.211        192.168.2.1     1390 0x80000001 0x897e
0.0.7.211        192.168.2.2     1354 0x80000001 0x9b69
                    Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID    ADV Router      Age  Seq#       CkSum  Prefix   Reference
0.0.0.1          192.168.2.1     1389 0x80000005 0x7e2e     1   Router-LSA
0.0.0.2          192.168.2.1     1389 0x80000001 0x22cb     1   Network-LSA
0.0.0.1          192.168.2.3     1306 0x80000002 0xd0d7     1   Router-LSA
```

Displayed information's Explanations
Link-LSA (Interface Vlan1) Link LSA messages of interface Vlan1
Router-LSA (Area 0.0.0.0) Router LSA messages in Area 0
Network-LSA (Area 0.0.0.0) Network LSA in Area 0
Intra-Area-Prefix-LSA (Area 0.0.0.0) Intra-domain Prefix LSA in Area 0

34.32 show ipv6 ospf interface

Command: show ipv6 ospf interface *<ifname>*|vlan *<vlan-id>*

Function: Display the OSPF interface messages.

Parameter: *<interface> is the* name of the interface.

Default: Not displayed

Command Mode: All modes

Example:

Loopback is up, line protocol is up

```
OSPFv3 not enabled on this interface
Vlan1 is up, line protocol is up
  Interface ID 2003
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2001:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Backup Designated Router (ID) 192.168.2.3
      Interface Address fe80::203:fff:fe01:d28
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
Vlan2 is up, line protocol is up
  Interface ID 2004
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2000:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 192.168.2.1
      Interface Address fe80::203:fff:fe01:429e
    Backup Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
```

Displayed information Explanations
Vlan1 is up, line protocol is up

Let the interface up both logically and physically
IPv6 Prefixes fe80::203:fff:fe01:257c/64 (Link-Local Address) 2001:1:1::1/64 IPv6 address of the interface and the length of the prefix
OSPFv3 Process (*null*) Ospfv3 process the interface belongs
Area 0.0.0.1 Area the interface belongs
Instance ID 0 Instance ID is 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10 Process ID; Router ID; Network Type; Cost
Transmit Delay is 1 sec, State DR, Priority 1 LAS transmission delay on the interface; state; electing the priority of the layer 3 switch.
Designated Router (ID) 192.168.2.2 Interface Address fe80::203:fff:fe01:257c Specifying layer 3 switch
Backup Designated Router (ID) 192.168.2.3 Interface Address fe80::203:fff:fe01:d28 Back up designated layer 3 switch
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:10 OSPF protocol timer; including hello packet, poll interval packets, router dead, router retransmission.
Neighbor Count is 1, Adjacent neighbor count is 1 Numbers of the adjacent layer 3 switch; number of the layer 3 switches established with neighbor relation

34.33 show ipv6 ospf neighbor

Command: show ipv6 ospf [<*tag*>] neighbor [<*neighbor_id*> | <ifname> detail | detail]

Function: Show OSPF adjacent point messages.

Parameter: <*tag*> is process tag, which is a character string

<*neighbor_id*> is the neighbor ID shown in IPv4 address format

detail: Show neighbor details

<*ifname*> name of the interface

Default: Not displayed

Command Mode: All modes

Usage Guide: OSPF neighbor state can be checked by viewing the output of this command.

Example:

```
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
192.168.2.3       1   Full/Backup     00:00:29    Vlan1      0
192.168.2.1       1   Full/DR         00:00:38    Vlan2      0            Vlan1
```

Displayed information Explanation
Neighbor ID Neighbor ID
Instance ID Instance ID
Address IP address of neighboring layer 3 switch
Interface Interface the neighbor belongs
State Neighbor relationship state
Pri Priority

34.34 show ipv6 ospf route

Command: show ipv6 ospf [<*tag*>] route

Function: Show the OSPF route table messages.

Parameter: <*tag*> is the processes tag, which is a character string.

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf route
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
O  2000:1:1::/64                                10
     directly connected, Vlan2
O  2001:1:1::/64                                10
     directly connected, Vlan1
O  3000:1:1::/64                                20
     via fe80::203:fff:fe01:429e, Vlan2
O  3003:1:1::/64                                20
     via fe80::203:fff:fe01:d28, Vlan1
```

34.35 show ipv6 ospf redistribute

Command: show ip ospf v6 [<*process-tag*>] redistribute

Function: To display the routing message redistributed from external process of OSPF.

Parameter: IPv6 OSPF is the tag ID, to display all routing messages redistributed from external process of IPv6 OSPF if there is no parameter.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: None.

Example:

```
Switch#show ipv6 ospf redistribute
        ospf process abc redistribute information：
          ospf process def
          bgp
        ospf process def redistribute information：
          ospf process abc
```

```
Switch#show ipv6 ospf abc redistribute
        ospf process abc redistribute information：
          ospf process def
          bgp
```

34.36 show ipv6 ospf topology

Command: show ipv6 ospf [<*tag*>] topology [area <*area-id*>]

Function: Show messages of OSPF topology.

Parameter: <*tag*> is the processes tag, which is a character string.

<*area-id*> is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address.

Default: Not displayed.

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID          Bits   Metric      Next-Hop              Interface
192.168.2.1               10          192.168.2.1           Vlan2
192.168.2.2               --
192.168.2.3               10          192.168.2.3           Vlan1
```

34.37 show ipv6 ospf virtual-links

Command: show ipv6 ospf [<*tag*>] virtual-links

Function: Show OSPF virtual link messages.

Parameter: <*tag*> is the processes tag, which is a character string.

Default: Not displayed.

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface Vlan1, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

34.38 show ipv6 route process-detail

Command: show ipv6 route [database] process-detail

Function: Display the IP routing table with specific process ID or Tag.

Parameters: The parameter of database means displaying all the routers, no parameter means only displaying effective routers.

Command Mode: Admin mode and configure mode.

Usage Guide: None.

Example:

```
Switch#show ipv6 route database process-detail
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*> ::1/128 via ::, Loopback, 00:29:53
O     2001::/64 [110/10] via ::, Vlan1, 00:01:07 ,process aaa
C*> 2001::/64 via ::, Vlan1, 00:02:54
O*> 2006::/64 [110/10] via ::, Vlan1, 00:01:07, process aaa
O*> 2008::/64 [110/20] via fe80::203:fff:fe01:2542, Vlan1, 00:00:54, process bbb
```

34.39 timers spf

Command: timers spf <*spf-delay*> <*spf-holdtime*>

no timers spf

Function: Adjust route calculation timer value. The "**no timers spf**" restores the relevant value to default.

Parameter: <*spf-delay*> 5 seconds by default

<*spf-holdtime*> 10 seconds by default

Command Mode: OSPFv3 protocol mode

Usage Guide: In this command the delay time between receiving topology change and SPF calculation, and further configured the hold time between two discontinuous SPF calculations.

Example:

```
Switch # config terminal
```

```
Switch (config)# router ipv6 ospf
```

```
Switch(config-router)#timers spf 5 10
```

Chapter 35 Commands for BGP and MBGP4+

35.1 address-family

Command: address-family <*AFI*> <*SAFI*>

Function: Enter address-family mode.

Parameter: <*AFI*> address-family, such as IPv4、IPv6、VPNv4, etc ;

<*SAFI*>: sub address-family, such as unicast、multicast

Default: None.

Command Mode: BGP routing mode

Usage Guide: Since the BGP-4 supports multi-protocol, it is available to get different configuration for each address-family. Actually the configuration outside address-family mode is configuring the default address-family (normally IPv4 unicast). To configure non default mode, enter this address-family mode.

Example:

Switch(config-router)# address-family ipv4 unicast

35.2 address-family ipv4

Command: address-family ipv4 {multicast | unicast | vrf<vrf-name>}

no address-family ipv4 vrf <*vrf-name*>

Function: Enter BGP VRF address-family mode. The no command deletes the configuration of the address-family.

Parameter: <*vrf-name*> specifies the name of VPN routing/forwarding instances.

Command Mode: BGP Route Mode.

Usage Guide: To support VPN, VRF has to be enabled on the border routers; to realize VPN, create neighbors for BGP with the VRF address family on the private network, and with VPNv4 address-family on the public network. Configuration performed with this command to specific VRF, is independent from IPv4 unicast address-family. The VRF configuration is performed by using ip vrf <NAME> command under global mode. The address-family configuration is only available after the VRF RD is set.

Example: In the example below a VRF name DC1 is created with RD at 100: :10, and then enter the BGP address-family for its configuration.

Switch(config)#ip vrf DC1
Switch(config-vrf)#rd 100:10
Switch(config-vrf)#exit
Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf DC1
Switch(config-router-af)#

35.3 address-family vpnv4

Command: address-family vpnv4

Function: Enter the BGP VPNv4 address family mode.

Parameter: None.

Command Mode: BGP route mode.

Usage Guide: To support VPN, VRF has to be enabled on the border routers; to realize VPN, create neighbors for BGP with the VRF address family on the private network, and with VPNv4 address-family on the public network. When configuring VPNv4 address-family with this command, IPv4 unicast address connection is available. Its neighbor configuration could be the same with IPv4 unicast only by using neighbor A.B.C.D activate on this neighbor to enable this address-family.

Example:

Switch(config)#router bgp 100
Switch(config-router)#address-family vpnv4
Switch(config-router-af)#

35.4 aggregate-address

Command: aggregate-address *<ip-address/M>* [summary-only] [as-set]

no aggregate-address *<ip-address/M>* [summary-only] [as-set]

Function: Configure the aggregate-address. The "**no aggregate-address *<ip-address/M>* [summary-only] [as-set]**" command deletes the aggregate-address.

Parameter: *<ip-address/M>*: IP address, length of mask.

[summary-only]: Send summary only ignoring specific route.

[as-set]: Show AS on the path in list, each AS is shown once.

Default: No aggregate configuration.

Command Mode: BGP route mode

Usage Guide: Address aggregation reduces spreading routing messages outside. Use summary-only option so to spread aggregate route to the neighbors without spreading specific route. as-set option will list AS from each route covered by the aggregation only once without repeat.

Example:

Switch(config-router)#aggregate-address 100.1.0.0/16 summary-only
Switch(config-router)#aggregate-address 100.2.0.0/16 summary-only as-set

Switch(config-router)#aggregate-address 100.3.0.0/16 as-set

Related Command: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

35.5 bgp aggregate-nexthop-check

Command: bgp aggregate-nexthop-check

no bgp aggregate-nexthop-check

Function: Configures whether BGP checks all the route next-hop in aggregating. The "**no bgp aggregate-nexthop-check**" command cancels this configuration, namely not check the next-hop accordance of aggregate route.

Parameter: None.

Default: No nexthop checked during aggregating.

Command Mode: Global mode

Usage Guide: When check is enabled, the aggregate will not be performed if the next-hop of the covered routes are not in accordance. When checking is disabled, all covered route will be aggregated into the aggregate route.

Example:

Switch(config)#bgp aggregate-nexthop-check

Relevant Command: aggregate-address, no aggregate-address

35.6 bgp always-compare-med

Command: bgp always-compare-med

no bgp always-compare-med

Function: Configures If MED comparation is always performed. The "**no bgp always-compare-med**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally the BGP compares the MED only when the AS is the same. By using this configuration, MED of routes from different AS source will also be compared.

Example: The AS (200) receives the same route prefix form the two AS (100 and 300) carrying different MED, configure the MED comparison is always performed.

Switch(config-router)#bgp always-compare-med

35.7 bgp bestpath as-path ignore

Command: bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Function: Set to ignore the AS-PATH length. The "**no bgp bestpath as-path ignore**" command cancels this configuration.

Parameter: None.

Default: Not set.

Command Mode: BGP route mode

Usage Guide: Length of AS-PATH will be compared in BGP pathing, and its length can be ignored by using this configuration.

Example:

Set to ignore the AS-PATH length:

Switch(config)#router bgp 200
Switch(config-router)#bgp bestpath as-path ignore

Related Command: bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid, no bgp bestpath med

35.8 bgp bestpath compare-confed-aspath

Command: bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Function: Set to concern the confederation AS-PATH length. The "**no bgp bestpath compare-confed-aspath**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally only the length of external AS-PATH will be compared in BGP pathing. By using this configuration, lengths of AS inner confederation AS-PATH will be compared at the same time.

Example:

Switch(config-router)#bgp bestpath compare-confed-aspath

35.9 bgp bestpath compare-routerid

Command: bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Function: Compare route ID; the "**no bgp bestpath compare-routerid**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally the first arrived route from the same AS (with other conditions equal) will be chosen as the best route. By using this command, source router ID will also be compared.

Example: Device（10.1.1.66, AS200）receives the same route prefix from two devices （10.1.1.64 and 10.1.1.68）of the same AS (100), configure the device to compare route ID.

```
Switch(config-router)#bgp bestpath compare-routerid
```

Related Command: bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath med

35.10 bgp bestpath med

Command: bgp bestpath med {[confed] [missing-as-worst]}

no bgp bestpath med {[confed] [missing-as-worst]}

Function: Configure whether the MED attributes should be compared in the confederation path and the treatment when MED is unavailable. The "**no bgp bestpath med {[confed] [missing-as-worst]}**" command cancels this configuration.

Parameter: [confed]: Compare MED in the confederation path.

[missing-is-worst]: Consider as max MED value when missing.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Choose whether MED is compared among confederations by this command. If MED is missing, it is considered max when missing-is-worst or else 0.

Example:

```
Switch(config-router)#bgp bestpath med confed missing-as-worst
```

Relevant Commands: bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid

35.11 bgp client-to-client reflection

Command: bgp client-to-client reflection

no bgp client-to-client reflection

Function: Configures whether the route reflection is performed. The "**no bgp client-to-client reflection**" cancels this configuration.

Parameter: None.

Default: Reflection defaulted when client is configured.

Command Mode: BGP route mode

Usage Guide: After configured reflection client with neighbor {<ip-address>|<TAG>} route-reflector-client, the router performs routing reflection in default condition. The NO form of this command cancels the route reflection among CLIENT, (reflection among Clients and non-CLIENT is not disturbed).

Example:

Switch(config-router)#no bgp client-to-client reflection

Relevant Commands: neighbor route-reflector-client, no neighbor route-reflector-client

35.12 bgp cluster-id

Command: bgp cluster-id {<*ip-address*>|<*01-4294967295*>}

no bgp cluster-id {[<*ip-address*>]|<*0-4294967295*>}

Function: Configure the route reflection ID during the route reflection. The "**no bgp cluster-id {[<*ip-address*>]|<*0-4294967295*>}**" command cancels this configuration.

Parameter: <*ip-address*>|<*1-4294967295*>: cluster-id which is shown in dotted decimal notation or a 32 digit number.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: A cluster consists of one routing reflector and its clients in an area. However in order to increase the redundancy level, sometime more than one routing reflectors may be deployed in one area. Router-id is for identifying the router exclusively in an area, and cluster-id is required for two or more reflector identification.

Example:

Switch(config-router)#bgp cluster-id 1.1.1.1

Related Command: neighbor route-reflector-client

35.13 bgp confederation identifier

Command: bgp confederation identifier *<as-id>*

no bgp confederation identifier [*<as-id>*]

Function: Create a confederation configuration. The "**no bgp confederation identifier [*<as-id>*]**" command deletes a confederation.

Parameter: ID number of the confederation AS.

Default: No confederation.

Command Mode: BGP route mode

Usage Guide: Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Create large AS number with this command.

Example:

Switch(config-router)# bgp confederation identifier 600

Related Command: bgp confederation peers, no bgp confederation peers

35.14 bgp confederation peers

Command: bgp confederation peers <as-id> [<as-id>..]

no bgp confederation peers *<as-id>* [*<as-id>..*]

Function: Add/delete one or several AS to a confederation.

Parameter: ID numbers of the AS included in the confederation, which could be multiple.

Default: No members.

Command Mode: BGP route mode.

Usage Guide: Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Use this command to add/delete confederation members.

Example:

Switch(config-router)# bgp confederation identifier 600
Switch(config-router)#bgp confederation peers 100 200

35.15 bgp dampening

Command: bgp dampening [*<1-45>*] [*<1-20000> <1-20000> <1-255>*] [*<1-45>*]

no bgp dampening

Function: Configure the route dampening.The "**no bgp dampening**" command cancels the route dampening function.

Parameter: *<1-45>*: Respectively the penalty half-lives of accessible and inaccessible route, namely the penalty value is reduced to half of the previous value, in minutes.

<1-20000>: Respectively the penalty reuse border and restrain border.

<1-255>: Maximum restrain route time, in minutes.

Default: Half-life of accessible route is 15 minutes, 15 minutes for inaccessible. The restrain border is 2000, reuse border is 750, and maximum restrain time is 60 minutes.

Command Mode: BGP Route Mode.

Usage Guide: Abundant route update due to unstable route could be reduced with route dampening technology, of which the algorithm is lay penalty on the route when the route fluctuates, and when penalty exceeds the restrain border this route will no longer be advertised. The penalty value will be reduced by time by the half-life index regulation if the route keeps stable and finally be advertised again when the penalty falls below the border or the restrain time exceeds the maximum restrain time. This command is for enabling/disabling the route dampening and configuring its parameters.

Example: Enable the route dampening and use the parameter configuration by default.

```
Switch(config-router)# bgp dampening
```

35.16 bgp default

Command: bgp default {ipv4-unicast|local-preference <*0-4294967295*>}

no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}

Function: Set the BGP defaults, the "**no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}**" command cancels this configuration.

Parameter:<*0-4294967295*>: Default local priority.

Default: The IPv4 unicast is default enabled when BGP is enabled. The default priority is 100.

Command Mode: BGP route mode.

Usage Guide: IPv4 unicast address-family is default enabled in BGP. Cancel this setting with no bgp default ipv4-unicast command so to not enable this address-family in default. Default local priority can be configured through bgp default local-preference command.

Example:

Configure in 10.1.1.66:

```
Switch(config)#router bgp 200

Switch(config-router)# bgp default local-preference 500
```

35.17 bgp deterministic-med

Command: bgp deterministic-med

no bgp deterministic-med

Function: Use the best MED for the same prefix in the AS to compare with other AS. The "**no bgp deterministic-med**" cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally if same prefix routes from several paths, each path will be compared. With this configuration, the system will only use the path with the smallest MED in the AS (when other main attributes equal) to compare with other AS. After the best one is elected, select the path among AS with no regard to MED value.

Example:

```
Switch(config-router)#bgp deterministic-med
```

35.18 bgp enforce-first-as

Command: bgp enforce-first-as

no bgp enforce-first-as

Function: Enforces the first AS position of the route AS-PATH contain the neighbor AS number or else disconnect this peer when the BGP is reviving the external routes. The "**no bgp enforce-first-as**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: This command is usually for avoiding unsafe or unauthenticated routes.

Example:

```
Switch(config-router)#bgp enforce-first-as
```

35.19 bgp fast-external-failover

Command: bgp fast-external-failover

no bgp fast-external-failover

Function: Fast reset when the BGP neighbor connection varies at the interface other than wait for TCP timeout. The "**no bgp fast-external-failover**" command cancels this configuration.

Parameter: None.

Default: Configured.

Command Mode: BGP route mode

Usage Guide: This command is for immediately cutting of the neighbor connection when the interface is down.

Example:

```
Switch(config-router)# bgp fast-external-failover
```


35.20 bgp inbound-route-filter

Command: bgp inbound-route-filter

no bgp inbound-route-filter

Function: The bgp do not install the RD routing message which does not exist locally. The "**no bgp inbound-route-filter**" command means the RD will be installed with no regard to the local existence of the RD.

Parameter: None.

Command Mode: BGP route mode.

Usage Guide: Normally when the switch plays as PE, whether the route bgp acquired from VPN is saved in BGP depends on if the VRF configured in this PE has got matched information. With the "**no bgp inbound-route-filter**" command the BGP will save the routing message with no regard to the matched information.

Example:

Switch(config)#router bgp 100
Switch(config-router)#no bgp inbound-route-filter

35.21 bgp inbound-max-route-num

Command: bgp inbound-max-route-num <0-500000>

no bgp inbound-max-route-num

Function: Set the number limit of routers learnt by the bgp process from its neighbors.

Parameters: The number limit of routers, ranging from 0 to 500000.

Default: The number limit is 50000 by default.

Command Mode: BGP routing mode and address family mode

Usage Guide: Limit the number of routers learnt by the bgp process from its neighbors with this command.

Example: The following configuration will limit max number of routers that the bgp process receives from its neighbors as 20000.

Switch(config-router)# bgp inbound-max-route-num 20000

35.22 bgp log-neighbor-changes

Command: bgp log-neighbor-changes

no bgp log-neighbor-changes

Function: Output log message when BGP neighbor changes. The "**no bgp log-neighbor-changes**" command cancels this configuration.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Can display neighbor change messages on the monitor.

Example:

```
Switch(config-router)# bgp log-neighbor-changes
```

35.23 bgp network import-check

Command: bgp network import-check

no bgp network import-check

Function: Set whether check the IGP accessibility of the BGP network route or not. The "**no bgp network import-check**" command sets to not checking the IGP accessibility.

Parameter: None.

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Checking the IGP accessibility of the route advertised by BGP is to check the existence of next-hop and its IGP accessibility.

Example:

```
Switch(config-router)# bgp network import-check
```

35.24 bgp rfc1771-path-select

Command: bgp rfc1771-path-select

no bgp rfc1771-path-select

Function: After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, or comparing the internal METRIC.

Parameter: None.

Default: Following

Command Mode: Global mode

Usage Guide: After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, when different AS exist, which should be perform without this attribute set.

Example:

Switch(config)# bgp rfc1771-path-select
Switch(config)# no bgp rfc1771-path-select

35.25 bgp rfc1771-strict

Command: bgp rfc1771-strict

no bgp rfc1771-strict

Function: Set whether strictly follows the rfc1771 restrictions. The "**no bgp rfc1771-strict**" command set to not strictly following.

Parameter: None.

Default: Not following rfc 1771 restrictions.

Command Mode: Global mode

Usage Guide: With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc will be regarded as IGP (internal generated), or else as incomplete.

Example:

Switch(config)# bgp rfc1771-strict
Switch(config)# no bgp rfc1771-strict

35.26 bgp router-id

Command: bgp router-id <*A.B.C.D*>

no bgp router-id [<A.B.C.D>]

Function: Configure the router ID manually. The "**no bgp router-id [<A.B.C.D>]**" cancels this configuration.

Parameter: <*A.B.C.D*>: Router ID.

Default: Automatically acquire router ID.

Command Mode: BGP route mode

Usage Guide: Manually set the router ID with this command.

Example:

Switch(config-router)# bgp router-id 1.1.1.1

35.27 bgp scan-time

Command: bgp scan-time <*0-60*>

no bgp scan-time [<*0-60*>]

Function: Set the time interval of the periodical next-hop validation; the "**no bgp scan-time [<*0-60*>]**" command restores to the default value.

Parameter: <*0-60*>: Validation time interval.

Default: Default interval is 60s.

Command Mode: BGP route mode

Usage Guide: Validate the next-hop of BGP route, this command is for configuring the interval of this check. Set the parameter to 0 if you don't want to check.

Example:

```
Switch(config-router)# bgp scan-time 30
```

35.28 clear ip bgp

Command: clear ip bgp [view <*NAME*>] {<*>|<*as-id*>| external|peer-group <*NAME*>|<*ip-address*>} [<*ADDRESS-FAMILY*>] [in [prefix-filter] |out|soft [in|out]]

Function: Clear up BGP links or states.

Parameter: *: all.

<as-id>: AS number.

<NAME>: Respectively BGP instance name and peer group name.

<ip-address>: IP address.

<ADDRESS-FAMILY>: Address family, such as "ipv4 unicast".

Default: None.

Command Mode: Admin mode

Usage Guide: Clearing up BGP state in different parameters (such as AS number, peer group name, IPv4 address, address-family, external neighbor), or the inbound or outbound messages. Also it is optional to use the saved ORF as soft reconfiguration, or use the soft in|out commands for in or out soft reconfiguration if it is already set.

Example:

When soft reconfiguration is set, use this command for soft reconfiguration.

```
Switch# clear ip bgp * soft in
```

Will clear up all established connections.

```
Switch# clear ip bgp *
```

35.29 clear ip bgp dampening

Command: clear ip bgp [<*address-family*>] dampening [<ip-address>|<ip-address/M>]

Function: Used for resetting BGP routing dampening.

Parameter: <*address-family*>: address-family, such as “ipv4 unicast”.

<*ip-address*>: IP address.

<*ip-address/M*>: IP address and mask.

Default: None.

Command Mode: Admin mode

Usage Guide: It is possible to clear BGP routing dampening messages and state by different parameters (such as address-family or IPv4 address).

Example:

```
Switch#clear ip bgp ipv4 unicast dampening
```

Related Command: bgp dampening

35.30 clear ip bgp flap-statistics

Command: clear ip bgp [<*address-family*>] flap-statistics [<*ip-address*>|<*ip-address/M*>]

Function: For resetting BGP routing dampening statistics messages.

Parameter: <*address-family* >: address-family such as “ipv4 unicast”.

<*ip-address*>: IP address.

<*ip-address/M*>: IP address and mask.

Default: None.

Command Mode: Admin mode.

Usage Guide: It is possible to clear BGP routing dampening statistic messages and state by different parameters (such as address-family or IPv4 address).

Example:

```
Switch#clear ip bgp ipv4 unicast flap-statistics
```

35.31 debug bgp

Command: debug bgp [<*MODULE*>|all]

no debug bgp [<*MODULE*>|all]

Function: For BGP debugging. The “**no debug bgp [<*MODULE*>|all]**” command closes the BGP debugging messages

Parameter: <*MODULE*>: BGP module names, including dampening、events、filters、fsm、keepalives、nsm、updates, etc.

Default: None

Command Mode: Admin mode and global mode

Usage Guide: For monitoring BGP events and the encountered errors, warning messages.

Example:

Switch#debug bgp all

35.32 debug bgp redistribute message send

Command: debug bgp redistribute message send

no debug bgp redistribute message send

Function: To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPF and RIP to BGP. The no command will disable the debugging switch.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch# debug bgp redistribute message send
Switch# no debug bgp redistribute message send

35.33 debug bgp redistribute route receive

Command: debug bgp redistribute route receive

no debug bgp redistribute route receive

Function: To enable debugging switch of received messages from NSM for BGP. The no form of this command will disable debugging switch of received messages from NSM for BGP.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

Switch#debug bgp redistribute route receive

```
Switch#no debug bgp redistribute route receive
```

35.34 debug ipv6 bgp redistribute message send

Command: debug ipv6 bgp redistribute message send

no debug ipv6 bgp redistribute message send

Function: To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPFv3 and others to MBGP4+. The no command will disable the debugging switch.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

```
Switch# debug ipv6 bgp redistribute message send
```

35.35 debug ipv6 bgp redistribute route receive

Command: debug ipv6 bgp redistribute route receive

no debug ipv6 bgp redistribute route receive

Function: To enable debugging switch of received messages from NSM for MBGP4+. The no form of this command will disable debugging switch of received messages from NSM for MBGP4+.

Parameter: None.

Default: Close the debug by default.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

```
Switch# debug ipv6 bgp redistribute route receive

Switch# no debug ipv6 bgp redistribute route receive
```

35.36 distance

Command: distance <1-255> <ip-address/M> [<WORD>]

no distance *<1-255>* *<ip-address/M>* [*<WORD>*]

Function: Set the manage distance of the routing prefix. The "**no distance *<1-255>* *<ip-address/M>* [*<WORD>*]**" command restores to the default value.

Parameter: *<1-255>*: Manage distance.

<ip-address/M>: Routing prefix.

<WORD>: Access-list name.

Default: Not set.

Command Mode: BGP route mode

Usage Guide: Set the manage distance for specified BGP route as the path selecting basis.

Example:

```
Switch(config-router)# distance 90 10.1.1.64/32
```

35.37 distance bgp

Command: distance bgp *<1-255> <1-255> <1-255>*

no distance bgp [*<1-255> <1-255> <1-255>*]

Function: Set the BGP protocol management distance. The "**no distance bgp [*<1-255> <1-255> <1-255>*]**" command restores the manage distance to default value.

Parameter: *<1-255>* Respectively the EBGP, IBGP and LOCAL manage distance of the BGP.

Default: Default EBGP is 20, others are 200.

Command Mode: BGP route mode

Usage Guide: Set the manage distance for BGP routing as the NSM path selecting basis.

Example: Set the manage distance for BGP routing as 15, the manage distance for IBGP and local routing as 150.

```
Switch(config-router)# distance bgp 15 150 150
```

35.38 exit-address-family

Command: exit-address-family

Function: Exit the BGP address-family mode.

Parameter: None.

Default: None.

Command Mode: BGP address-family mode

Usage Guide: Use this command to exit the mode so to end the address-family configuration when configuring address-family under BGP.

Example:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv4 unicast
```

Switch(config-router-af)# exit-address-family
Switch(config-router)#

Related Command: address-family

35.39 import map

Command: import map <map-name>

no import map *<map-name>*

Function: Use this command to configure the route-map regulations when introducing routes into VRF.

Parameter: *<map-name>* is the route-map name used.

Command Mode: VRF mode.

Usage Guide: Use the route map command route-map NAME permit|deny <1-65535> to create the route-map and establish the regulations. Using this command will apply regulations to the route introducing of this VRF.

Example:

Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
Switch(config-map)#set weight 655 Reconfiguring VRF DC1 with this route-map
Switch(config-map)#exit
Switch(config)#ip vrf DC1
Switch(config-af)#rd 100:10
Switch(config-af)#route-target both 100:10
Switch(config-af)#import map map1
Switch#show ip bgp vpn all Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 100:10 (Default for VRF DC1) *> 11.1.1.0/24 11.1.1.64 0 0 200 ? *>i15.1.1.0/24 10.1.1.68 0 100 655 300 ? *> 20.1.1.0/24 11.1.1.64 0 0 200 ? *>i100.1.1.0/24 10.1.1.68 0 100 655 300 ? Route Distinguisher: 100:10

*>i15.1.1.0/24	10.1.1.68	0	100	0 300 ?
*>i100.1.1.0/24	10.1.1.68	0	100	0 300 ?

As we can see, the weight of the route from the VPN changes to 655 after introduced into VRF DC1.

35.40 ip as-path access-list

Command: ip as-path access-list <.LINE> {<permit>|<deny>} <LINE>

no ip as-path access-list <*.LINE*> {<*permit*>|<*deny*>} <*LINE*>

Function: Configure the AS-PATH access-list. The "**no ip as-path access-list <*.LINE*> {<*permit*>|<*deny*>} <*LINE*>**" command deletes this access-list.

Parameter: <*.LINE*>: name of access-list.

<*LINE*>: matched strings in the AS-PATH.

Default: None.

Command Mode: Global mode.

Usage Guide: Use this command to configure the access-list related to AS-PATH, so to supply the conditions for pass/filter.

Example:

```
Switch(config)#ip as-path access-list ASPF deny ^100$
```

35.41 ip community-list

Command: ip community-list {<*LISTNAME*> | <*1-199*> | [expanded <*WORD*>] | [standard <*WORD*>]} {deny | permit} <*.COMMUNITY*>

no ip community-list {<*LISTNAME*> | <*1-199*> | [expanded <*WORD*>] | [standard <*WORD*>]} [{deny | permit} <*.COMMUNITY*>]

Function: Configure the community-list. The "**no ip community-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} [{deny|permit} <*.COMMUNITY*>]**" command deletes the community list.

Parameter: <*LISTNAME*>: name of community list.

<*1-199*>: Standard or extended community number.

<*WORD*>: Standard or extended community number.

<*.COMMUNITY* >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.

Default: None.

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search.

Example:

Switch(config)# ip community-list LN permit 100:10

35.42 ip extcommunity-list

Command: ip extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>

no ip extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>

Function: Configure the extended community-list. The "**no ip extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>**" command is for deleting the extended community list.

Parameter: <*LISTNAME*>: name of community-list.

<*1-199*>: Standard or extended community number.

<*WORD*>: Standard or extended community number.

<*.COMMUNITY* >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.

Default: None.

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search.

Example:

Switch(config)# ip extcommunity-list LN permit 100:10

35.43 neighbor activate

Command: neighbor {<*ip-address*>|<*TAG*>} activate

no neighbor {<*ip-address*>|<*TAG*>} activate

Function: Configure the address family routing which do or do not switch specific address-family with BGP neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} activate**" command is for setting the route which do not switch the specified address family.

Parameter: <*ip-address*>: IP address of the neighbor.

<*TAG*>: Name of peer group.

Default: Enable the routing switch of IP unicast address-family, and disable other address-families.

Command Mode: BGP route mode and address-family mode

Usage Guide: IP unicast is configured under BGP route mode. Configure whether specific

address-family is switched under address-family mode. If this option on any side between local side and partner is not enabled, the address-family route will not be acquired by the partner even if the corresponding address family routes acquired before will be cancelled after this option is disabled.

Example:

```
Switch(config-router)#neighbor 2002::2 activate
Switch(config-router)#address-family ipv4
Switch(config-router-af)#no neighbor 2002::2 activate
Switch(config-router-af)#
```

35.44 neighbor advertisement-interval

Command: neighbor {*<ip-address>*|*<TAG>*} advertisement-interval *<0-600>*

no neighbor {*<ip-address>*|*<TAG>*} advertisement-interval [*<0-600>*]

Function: Configure the update interval of specific neighbor route. The "**no neighbor {*<ip-address>*|*<TAG>*} advertisement-interval [*<0-600>*]**" command restores to default.

Parameter: *<ip-address>*: IP address of the neighbor.

<TAG>: Name of the peer group.

***<0-600>*:** Advertise interval, in seconds.

Default: Default IBGP is 5s, default EBGP is 30s.

Command Mode: BGP route mode and address-family mode

Usage Guide: Reduce this value will improve the route updating speed while also consumes more bandwidth.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20
Switch(config-router)#no neighbor 10.1.1.64 advertisement-interval
Switch(config-router)#
```

35.45 neighbor allowas-in

Command: neighbor {*<ip-address>*|*<TAG>*} allowas-in [*<1-10>*]

no neighbor {*<ip-address>*|*<TAG>*} allowas-in

Function: Configure the counts same AS is allowed to appear in the neighbor route AS table. The "**no neighbor {*<ip-address>*|*<TAG>*} allowas-in**" restores to not allow any repeat.

Parameter: *<ip-address>*: IP address of the neighbor.

<TAG>: Name of the peer group.

<1-10>: Allowed count of same AS number.

Default: In default conditions AS is not allowed repeating in the same route, and when set the repeat

count it is defaulted at 3 when <1-10> parameters not set.

Command Mode: BGP route mode and address family mode

Usage Guide: Normally BGP will not allow same AS number appears in the route more than one time. The system will deny a route when its AS number appears in the AS-PATH. However to support some special needs, especially the VPN support, the extended BGP allows the AS re-appear counts by configuration. This command is for configure the re-appear counts.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 allowas-in
```

35.46 neighbor attribute-unchanged

Command: neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]

no neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]

Function: Configure certain attributes which is kept unchanged for transmitting, namely the attribute transparent transmission. The "**no neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]**" command means the attribute transparent transmission is not performed.

Parameter: *<ip-address>*: IP address of the neighbor.

***<TAG>*:** Name of the peer group.

Default: No attribute transparent defined.

Command Mode: BGP route mode and address-family mode

Usage Guide: With this configuration specified route attributes will not change when transmitted to the specified neighbor. The BGP route mode is the IPv4 unicast configuration. No parameter refers to above three parameter are configured together.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 attribute-unchanged
```

35.47 neighbor capability

Command: neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

Function: Configure dynamic update between neighbors and the route refresh capability negotiation. The "**no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}**" command do not enable the specific capability negotiation.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of peer group.

Default: Not configure the dynamic update capability but the route refresh capability.

Command Mode: BGP route mode and address family mode.

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. The dynamic capability refers to when the address family negotiation changes, the connection don't have to be restarted. Route refresh refers to sending refresh request when configuring some soft reconfigurable attributes and the partner will retransmit the existing route to the originating side. With route refresh attribute, the connection will not have to be restarted but be refreshed with the clear ip bgp * soft in command.

Example:

Switch(config-router)#neighbor 10.1.1.64 capability dynamic
Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh

35.48 neighbor capability orf prefix-list

Command: neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}

no neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}

Function: Configure the out route filter capability negotiation between neighbors. The "**no neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}**" command set to not perform the negotiation.

Parameter: *<ip-address>*: Neighbor IP address.

***<TAG>*:** Name of peer group.

Default: ORF capability not configured.

Command Mode: BGP route mode and address-family mode

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. With this capability, the side configured with in prefix-list filter rules will transmit its own filter rules to the peer, the peer group will apply this rule as its own out rules, so to avoid sending route which will be denied by the partner.

Example:

Switch(config-router)#neighbor 10.1.1.66 capability orf prefix-list both

Relevant Commands: neighbor capability, no neighbor capability

35.49 neighbor collide-established

Command: neighbor {<*ip-address*>|<*TAG*>} collide-established

no neighbor {<*ip-address*>|<*TAG*>} collide-established

Function: Enable the collision check and settlement in the TCP connection collision. The "**no neighbor {<*ip-address*>|<*TAG*>} collide-established**" command disables the TCP connection collision settlement.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer.

Default: Disabled and Unavailable.

Command Mode: route mode and address family mode

Usage Guide: This command is for settling the problem that multi-connection among peers due to TCP connection collision. Connections created with this option on will always be check even at established state. And it will be checked if local side IP is larger than partner IP when collides. If yes, the original connection will be deleted, and if not the option will be configured to only checks when the connection originated from local side at open sent and open confirm state.

Example:

Switch(config-router)#neighbor 10.1.1.64 collide-established

35.50 neighbor default-originate

Command: neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]

no neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]

Function: Configures whether enables transmitting default route to the specific neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]**" command configures not sending default route to neighbors.

Parameter: <*ip-address*>: IP address of the neighbor.

<*TAG*>: Name of the peer.

<*WORD*>: Name of route map.

Default: Not sending default route.

Command Mode: BGP route mode and address-family mode

Usage Guide: With this option, the default route of local side will be transmitted to partner, or else not. It supplies with options of which one to supply the default route. if several neighbors of the partner supply default route, the best one will be elected according to path selecting principles. According to route mirror, it can be chosen when to send the default route.

Example: Set to transmit the local default route to neighbor 10.1.1.64

Switch(config-router)#neighbor 10.1.1.64 default-originate
Switch(config-router)#

Relevant Commands: route-map

35.51 neighbor description

Command: neighbor {*<ip-address>*|*<TAG>*} description *<.LINE>*

no neighbor {*<ip-address>*|*<TAG>*} description

Function: Configure the description string of the peer or peer group. The "**no neighbor {*<ip-address>*|*<TAG>*} description**" command deletes the configurations of this string.

Parameter: *<ip-address>*: Neighbor IP address.

<TAG>: Name of peer group.

<.LINE>: Description string consists of displayable characters less than 80.

Default: Description string is empty.

Command Mode: BGP route mode and address-family mode

Usage Guide: Configure the introduction of the peer or peer group.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 description tester

Switch(config-router)#
```

35.52 neighbor distribute-list

Command: neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}

no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}

Function: Configure the policy applied in partner route update transmission. The "**no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}**" command cancels the policy configuration.

Parameter: *<ip-address>*: Neighbor IP address.

<TAG>: Name of peer group.

<1-199>*|*<1300-2699>*|*<WORD>: Number or name of the access-list.

Default: Policy not applied.

Command Mode: BGP route mode and address-family mode

Usage Guide: Configure the policies with access-list command and apply this command on route sending and receiving. It will filter the update route from partner when use in mode, and will filter the route from local side to partner with out mode.

Example:

Configure the access-list

```
Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any

Switch(config)#access-list 101 permit ip any any

Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 10.1.1.66 distribute-list 101 out
```

Related Command: ip access-list

35.53 neighbor dont-capability-negotiate

Command: neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate

no neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate

Function: Set to not perform capability negotiate in creating connections. The "**no neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

Default: Capability negotiation performed.

Command Mode: BGP route mode and address-family mode

Usage Guide: As the negotiation is the default, it can be disabled with this configuration when it is known that the partner BGP version is old which don't support capability negotiation.

Example: Last addition capability negotiation will not be realized in the connection by configuring as follows.

```
Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate
```

35.54 neighbor ebgp-multihop

Command: neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]

no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]

Function: Configures the EBGP neighbors can existing in different segment as well as its hop count (TTL). The "**no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]**" set that the EBGP neighbors must be in the same segment.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

<1-255>: Allowed hop count.

Default: Must be in the same segment.

Command Mode: BGP route mode and address-family mode

Usage Guide: Without this command, EBGP peers are required to be in the same segment and after this command is configured, peer addresses may from different segments. The allowed hop count can be configured and will be 255 if not.

Example:

Three device 10.1.1.64(AS100) and 11.1.1.120(AS300) connected respectively to the two interface 10.1.1.66 and 10.1.1.100 of another device. IGP accessibilities of 10.1.1.64 and 11.1.1.120 on both side routes are ensured through static configuration. The neighbor relationship is established only after both side are configured as follows:

on 10.1.1.64

```
Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop
```

on 11.1.1.120

```
Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop
```

After this, switches in different segments will be able to create BGP neighbor relationship.

35.55 neighbor enforce-multihop

Command: neighbor {<*ip-address*>|<*TAG*>} enforce-multihop

no neighbor {<*ip-address*>|<*TAG*>} enforce-multihop

Function: Enforce the multihop connection to the neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} enforce-multihop**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of peer group.

Default: Not enforced.

Command Mode: BGP route mode and address-family mode

Usage Guide: In fact the direct route can not be enforced to multihop, however will be treated as a multihop connection with this configuration, namely the check originally only performed on IBGP and EBGP of non-direct routes will be performed on all after this attribute set. The nexthop direct connected check will not be performed at exit in enforce multihop conditions.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 enforce-multihop
```

35.56 neighbor filter-list

Command: neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}

no neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}

Function: Access-list control for AS-PATH. The "**no neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}**" cancels the AS-PATH access-list control.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of peer group.

<*LINE*>: AS-PATH access-list name configured through ip as-path access-list *<.LINE> <permit|deny> <LINE>.*

Default: Not configured.

Command Mode: BGP route mode and address list mode.

Usage Guide: After first configured the IP AS-PATH access-list, apply this option to specified neighbor will be able to send/receive routes with specified AS numbers in the AS list. Accepting or denying depends on the configuration of the access-list, while sending and receiving are configured by this command.

Example:

Configure the AS-PATH access control list, “ASPF” is the name of the access-list. The route with AS number of 100 will not be able to update to the partner due to the filter table control.

Switch(config)#ip as-path access-list ASPF deny 100
Switch(config)#router bgp 100
Switch(config-router)# redistribute static
Switch(config-router)neighbor 10.1.1.66 filter-list aspf out

Relevant Commands: ip as-path access-list

35.57 neighbor interface

Command: neighbor *<ip-address>* interface *<IFNAM>*

no neighbor *<ip-address>* interface *<IFNAM>*

Function: Specify the interface to the neighbor. The “**no neighbor *<ip-address>* interface *<IFNAM>***“of the command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address.

***<IFNAME>*:** Interface name, e.g. “Vlan 2”.

Default: Not configured.

Command Mode: BGP route mode and address-family mode

Usage Guide: Specifies the exit interface to the neighbor with this command. Interface destination accessibility should be ensured.

Example:

Switch(config-router)# neighbor 10.1.1.64 interface Vlan2

35.58 neighbor maximum-prefix

Command: neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]

no neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]

Function: Control the number of route prefix from the neighbor. The “**no neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]**” command cancels this configuration.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of the peer.

<1-4294967295>: Max prefix value allowed.

<1-100>: Percentage of the max value at which it warns.

<warning-only>: Warning only or not.

Default: Not limited.

Command Mode: BGP route mode and address-family mode

Usage Guide: Due to concerns of too much route updates from neighbors (e.g. attack), the max number of prefix acquired from a neighbor is limited, and will warns when the number hits certain rate. If the warning-only option is set, then there will be warning only, if not, the connection to the neighbor will be cut till clear the records with clear ip bgp command.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50
```

In above configuration, it warns when the number of route prefix reaches 6, and the connection will be cut when the number hit 13.

35.59 neighbor next-hop-self

Command: neighbor {*<ip-address>*|*<TAG>*} next-hop-self

no neighbor {*<ip-address>*|*<TAG>*} next-hop-self

Function: Ask the neighbor to point the route nexthop sent by the local side to local side. The "**no neighbor {*<ip-address>*|*<TAG>*} next-hop-self**" command cancels this configuration.

Parameter: ***<ip-address>***: Neighbor IP address.

<TAG>: Name of peer group.

Default: Not configured by default.

Command Mode: BGP route mode and address-family mode

Usage Guide: In the EBGP environment, the nexthop will automatically point to the source neighbor. However in IBGP environment, the nexthop remains the same for route in the same segment. If it is not broadcast network, errors will be encountered. This command is for force self as the nexthop of the neighbor under IBGP.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 next-hop-self
```

35.60 neighbor override-capability

Command: neighbor {<*ip-address*>|<*TAG*>} override-capability

no neighbor {<*ip-address*>|<*TAG*>} override-capability

Function: Whether enable overriding capability negotiation. The "**no neighbor {<*ip-address*>|<*TAG*>} override-capability**" command restores the capability negotiation.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

Default: Disabled.

Command Mode: BGP route mode

Usage Guide: With this attribute, error notify due to unsupported capability negotiation the neighbors required will not be sent.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 override-capability
```

Related Command: neighbor capability

35.61 neighbor passive

Command: neighbor {<*ip-address*>|<*TAG*>} passive

no neighbor {<*ip-address*>|<*TAG*>} passive

Function: Configure whether the connecting request is positively sent in the connection with specified neighbor; the "**no neighbor {<*ip-address*>|<*TAG*>} passive**" command restores to positively send the connecting request.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of peer group.

Default: Positively send the connecting request.

Command Mode: BGP route mode and address-family mode

Usage Guide: With this attribute set, the local side will not positively send the TCP connecting request after the neighbors are configured, but stays in listening mode waiting for the connecting request from partners.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 passive
```

After configured with this attribute and reestablishing the connection , the local side do not attempt to create connection but stays in ACTIVE state waiting for the TCP connection request from the partner.

35.62 neighbor peer-group (Creating)

Command: neighbor < *TAG*> peer-group

no neighbor < *TAG*> peer-group

Function: Create/delete a peer group. The "**no neighbor < *TAG*> peer-group**" command deletes a peer group.

Parameter: <*TAG*>: Name of the peer group of which the largest length contains 256 characters.

Default: No peer group.

Command Mode: BGP route mode and address-family mode

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Assign members to the peer group with neighbor <ip-address> peer-group <TAG> command.

Example:

Switch(config-router)#neighbor pg peer-group
Switch(config-router)#neighbor 10.1.1.64 peer-group pg
Switch(config-router)#neighbor pg remote-as 100

Related Command: neighbor peer-group (Configuring group members)

35.63 neighbor peer-group (Configuring group members)

Command: neighbor <*ip-address*> peer-group <*TAG*>

no neighbor <*ip-address*> peer-group <*TAG*>

Function: Assign/delete peers in the group. The "**no neighbor <*ip-address*> peer-group <*TAG*>**"command deletes the peers from the peer group.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of peer group.

Default: No peer group.

Command Mode: BGP route mode and address-family mode

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Create peer group with above command and assign members into the group with this command.

Example: Refer to above examples.

Related Command: neighbor peer-group (Creating)

35.64 neighbor port

Command: neighbor <*ip-address*> port <*0-65535*>

no neighbor <*ip-address*> port [<*0-65535*>]

Function: Specify the TCP port number of the partner through which the communication carries. The "**no neighbor <*ip-address*> port [<*0-65535*>]**" command restores the port number to default value.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

***<0-65535>*:** TCP port number.

Default: Default port number is 179.

Command Mode: BGP route mode and address-family mode

Usage Guide: This is a configuration when the partner may connect through ports not specified by BGP.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 port 1023
```

35.65 neighbor prefix-list

Command: neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*|*out*>}

no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*>|<*out*>}

Function: Configure the prefix restrictions applied in sending or receiving routes from specified neighbors.The "**no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*>|<*out*>}**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of the peer group.

<*LISTNAME*|*number*>: Name or sequence number of the prefix-list.

<*in*|*out*>: Direction on which the restrictions applied.

Default: No prefix restrictions applied.

Command Mode: BGP route mode and address-family mode

Usage Guide: Specify the prefix and its scope by configuring ip prefix-list and determines whether this scope is permitted or denied. Only the route with permitted prefix will be sent or received.

Example:

```
Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25
Switch(config)#router bgp 200
Switch(config-router)#redistribute static
Switch(config-router)neighbor 10.1.1.66 prefix-list prw out
```

35.66 neighbor remote-as

Command: neighbor {<*ip-address*>|<*TAG*>} remote-as <*as-id*>

no neighbor {<*ip-address*>|<*TAG*>} [remote-as <*as-id*>]

Function: Configure the BGP neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} [remote-as <*as-id*>]**" command is used for deleting BGP neighbors.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*as-id*>: Neighbor AS number ranging between 1-65535

Default: No neighbors

Command Mode: BGP route mode and address-family mode

Usage Guide: The BGP neighbors are completely generated through command configurations. A neighbor relationship can only be really established by mutual configuring. Partner AS number should be specified in configuration. The neighbor relationship can not be established when the AS number is incorrect. The partner AS number is the same with that of local side inside the AS.

Example:

Switch(config)#router bgp 200
Switch(config-router)# neighbor 10.1.1.64 remote-as 100

35.67 neighbor remove-private-AS

Command: neighbor {<*ip-address*>|<*TAG*>} remove-private-AS

no neighbor {<*ip-address*>|<*TAG*>} remove-private-AS

Function: Configures whether remove the private AS number when sending to the neighbor.The "**no neighbor {<*ip-address*>|<*TAG*>} remove-private-AS**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured

Command Mode: BGP route mode and address-family mode

Usage Guide: Configure this attribute to avoid assigning the internal AS number to the external AS sometimes. The internal AS number ranges between 64512-65535, which the AS number could not be sent to the INTERNET since it is not a valid external AS number. What removed here is private AS numbers of the totally private AS routes. Those who have private AS numbers while also have public AS numbers are not processed.

Example:

Switch(config-router)#neighbor 10.1.1.64 remove-private-AS

35.68 neighbor route-map

Command: neighbor {<*ip-address*>|<*TAG*>} route-map <*NAME*> {<*in*|*out*>}

no neighbor {<*ip-address*>|<*TAG*>} route-map <*NAME*> {<*in*|*out*>}

Function: Configure the route mapping policy when sending or receiving route. The "**no neighbor {<*ip-address*>|<*TAG*>} route-map <*NAME*> {<*in*|*out*>}**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*NAME*>: Name of route mapping

<*in*|*out*>: Direction of route mapping

Default: Not set

Command Mode: BGP route mode and address-family mode

Usage Guide: First it has to configure route mapping under global mode by creating a route map with route-map command and configure the match condition and actions, then the command can be applied.

Example:

```
Switch(config)#route-map test permit 5
Switch(config-route-map)#match interface Vlan1
Switch(config-route-map)#set as-path prepend 65532
Switch(config-route-map)#exit
Switch(config)#router bgp 200
Switch(config-router)#neighbor 10.1.1.64 route-map test out
```

35.69 neighbor route-reflector-client

Command: neighbor {<*ip-address*>|<*TAG*>} route-reflector-client

no neighbor {<*ip-address*>|<*TAG*>} route-reflector-client

Function: Configure the route reflector client. The "**no neighbor {<*ip-address*>|<*TAG*>} route-reflector-client**" command cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured.

Command Mode: BGP route mode and address-family mode

Usage Guide: The route reflection is used for reducing the peers when the internal IBGP routers inside AS are too much. The client only exchanges messages with route reflector while the reflector deals with message exchange among each client and other IBGP, EBGP routers. This command configures itself as the route reflector, while specific peer group is as its client. Note: this configuration is only available inside AS.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.66 remote 100
Switch(config-router)#neighbor 10.1.1.66 route-reflector-client
```

Switch(config-router)#neighbor 10.1.1.68 remote 100
Switch(config-router)#neighbor 10.1.1.68 route-reflector-client
Switch(config-router)#

Related Command: bgp client-to-client reflection, no bgp client-to-client reflection, bgp cluster-id

35.70 neighbor route-server-client

Command: neighbor {<*ip-address*>|<*TAG*>} route-server-client

no neighbor {<*ip-address*>|<*TAG*>} route-server-client

Function: Configure the route server client. The "**no neighbor {<*ip-address*>|<*TAG*>} route-server-client**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured

Command Mode: BGP route mode and address-family mode

Usage Guide: The route service is for reducing the peers when the router between AS is too much under EBGP environment. The server transparently transforms the routing messages to other clients with its client exchanges messages through route server.

Example:

Three routers : 10.1.1.64（AS100） and 10.1.1.68（AS300） respectively creates neighbor relationship with the connected 10.1.1.66（AS200）, the configuration is as follows:

Switch(config)#router bgp 200
Switch(config-router)#neighbor 10.1.1.64 remote-as 100
Switch(config-router)#neighbor 10.1.1.64 route-server-client
Switch(config-router)# neighbor 10.1.1.68 remote-as 300
Switch(config-router)# neighbor 10.1.1.68 route-server-client

35.71 neighbor send-community

Command: neighbor {<*ip-address*>|<*TAG*>} send-community [both|extended|standard]

no neighbor {<*ip-address*>|<*TAG*>} send-community [both|extended|standard]

Function: Configures whether sending the community attribute to the neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} send-community [both|extended|standard]**" command set to not sending.

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of peer group

[both|extended|standard]: Standard community only, extended community or both.

Default: Sending the community attributes.

Command Mode: BGP route mode and address-family mode

Usage Guide: The community attributes can be sent to the outside or not. By default of our company we set to sending while the default in standard protocol is not sending. By configuring this attribute community attributes will be carried when sending routing information's to the neighbors, or else not. Omission of the following choice will be equal to standard.

Example:

```
Switch(config-router)#no neighbor 10.1.1.66 send-community

Switch(config-router)#neighbor 10.1.1.66 send-community
```

35.72 neighbor shutdown

Command: neighbor {<*ip-address*>|<*TAG*>} shutdown

no neighbor {<*ip-address*>|<*TAG*>} shutdown

Function: Disconnect the neighbor connection. The "**no neighbor {<*ip-address*>|<*TAG*>} shutdown**" cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not disconnecting.

Command Mode: BGP route mode and address-family mode

Usage Guide: Directly disconnect/connect to a peer (group) without canceling the neighbor configuration.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 shutdown

```

35.73 neighbor soft-reconfiguration inbound

Command: neighbor {<*ip-address*>|<*TAG*>} soft-reconfiguration inbound

no neighbor {<*ip-address*>|<*TAG*>} soft-reconfiguration inbound

Function: Configures whether perform inbound soft reconfiguration; the "**no neighbor {<*ip-address*>|<*TAG*>} soft-reconfiguration inbound**" command set to not perform the inbound soft reconfiguration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not perform inbound soft reconfiguration.

Command Mode: The system saves the inbound messages in the buffer after the soft reconfiguration is

set, will applies as soon as it restarts so to reduce consumptions of switching with other routers. The command is only available when the route refresh capability is not enabled

Example:

Switch(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound

35.74 neighbor soo

Command: neighbor <ip-addr> soo <soo-val>

no neighbor <*ip-addr*> soo <*soo-val*>

Function: Configure the origin source from the neighbor route

Parameter: The neighbor IP address show in dotted decimal notation

<*soo-val*> is the origin source ,which the format is the same with RD

Command Mode: vrf mode

Usage Guide: If the user AS connects with several ISP devices, to avoid the user route returns to itself through P area, this attribute can be set. Once this attribute is set, it spreads with route. routes carrying SOO attributes will not be spreader to a neighbor configured with the attribute

Example:

Switch(config)#ROUTER BGP 100
Switch(config-router)#address-family ipv4 vrf DC1
Switch(config-router-af)# neighbor 11.1.1.64 remote 200
Switch(config-router-af)# neighbor 11.1.1.64 soo 100:10

After this attribute set, the switch will no longer spreads the route with 100:10 rt attribute to 11.1.1.64. (what have to be mentioned here is that the soo attribute will be judged together with other rt attributes, which means if the rt is configured with the same attribute, it will be regarded as the origin neighbor even if it's not the real origin source. As a matter of fact, the normal configured soo are a single configuration which is different from rt/rd and unique within the accessible scope. In this way can only the origin concept be exactly expressed)

35.75 neighbor strict-capability-match

Command: neighbor {<*ip-address*>|<*TAG*>} strict-capability-match

no neighbor {<*ip-address*>|<*TAG*>} strict-capability-match

Function: Configure whether strict capability match is required when establishing connections. The "**no neighbor {<*ip-address*>|<*TAG*>} strict-capability-match**" command set to not requiring strict match.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: No strict capability match configured.

Command Mode: BGP route mode and address-family mode

Usage Guide: With this command, the connection can only be established when the both side are perfectly matched on capabilities.

Example:

Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

35.76 neighbor timers

Command: neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>

no neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>

Function: Configure the KEEPALIVE interval and hold time; the "**no neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>**" command restores the defaults.

Parameter: <*ip-address*>Neighbor IP address

<*TAG*>: Name of peer group

<*0-65535*>: Respectively the KEEPALIVE and HOLD TIME

Default: Default KEEPALIVE time is 60s, while HOLD TIME is 240s.

Command Mode: BGP route mode and address-family mode

Usage Guide: Send KEEPALIVE interval and HOLD TIME intervals sent in the peer connection. The hold time is the time period for maintain the connection when no message is received from the partner (such as KEEPALIVE). And the connection will be closed after this hold time.

Example:

Switch(config-router)#neighbor 10.1.1.64 timers 50 200

Relevant Commands: neighbor timers connect, timers bgp, no timers bgp

35.77 neighbor timers connect

Command: neighbor {<*ip-address*>|<*TAG*>} timers connect <*0-65535*>

no neighbor {<*ip-address*>|<*TAG*>} timers connect [<*0-65535*>]

Function: Configure the connecting retry time interval. The "**no neighbor {<*ip-address*>|<*TAG*>} timers connect [<*0-65535*>]**" command restores the default value.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*0-65535*>: Retry interval

Default: 120s.

Command Mode: BGP route mode and address-family mode

Usage Guide: Configure the connecting time interval when connecting a peer. The NO form restores the default value.

Example:

Switch(config-router)#neighbor 10.1.1.64 timers connect 100

Related Command: neighbor timers

35.78 neighbor unsuppress-map

Command: neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>*

no neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>*

Function: Configure or cancel the unsurprising to conditions meet the specified route map. The "**no neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>***" command cancels this configuration.

Parameter: *<ip-address>*: Neighbor IP address.

<TAG>: Name of peer group.

<WORD>: Name of route-map.

Default: Not set.

Command Mode: BGP route mode

Usage Guide: This command is generally for route suppressed by the aggregated and summary-only conditions. Routes meet the route map conditions will still be send separately other than suppressed.

Example:

Switch(config-router)#neighbor 10.1.1.66 unsuppress-map rmp
Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255
Switch(config)#route-map rmp permit 5
Switch(config-route-map)#match ip next-hop 10

Route with nexthop as 10.1.1.100 will not be restrained.

35.79 neighbor update-source

Command: neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>*

no neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>*

Function: Configure the update source. The "**no neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>***"cancels this configuration

Parameter: *<ip-address>*: Neighbor IP address

<TAG>: Name of peer group

<IFNAME>: Name or IP of the interface

Default: Not configured, namely use nearest interface.

Command Mode: BGP route mode

Usage Guide: Specified update source is allowed to connect with any available interface which normally is the loop back interface. The NO forms restores to the nearest interface update source. Improper update source use may lead to neighbor connection unavailable, while the invalid interface causes problem which is also the reasons we use loop back interfaces. Note: the loop back interface should be maintained with its address accessibility to be able to establish connections when as the update source.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1
```

35.80 neighbor version 4

Command: neighbor {<*ip-address*>|<*TAG*>} version 4

Function: Configure the BGP version of the partner.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

4: Allowed BGP version, 4 only

Default: 4.

Command Mode: BGP route mode

Usage Guide: Only version 4 is supported so far, so whatever the configuration is the version remains at 4.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 version 4

Switch(config-router)#
```

35.81 neighbor weight

Command: neighbor {<*ip-address*>|<*TAG*>} weight <*0-65535*>

no neighbor {<*ip-address*>|<*TAG*>} weight [<*0-65535*>]

Function: Configure the route weight sent from the partner. The "**no neighbor {<*ip-address*>|<*TAG*>} weight [<*0-65535*>]**" command restores the default value.

Parameter: <*ip-address*>: Neighbor IP address.

<*TAG*>: Name of IP address.

<*0-65535*>: Weight.

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768.

Command Mode: BGP route mode

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768.

Usage Guide: The path selecting can be affected through the configuration of the weight. The weight is only relevant to the router which is not an attribute transmittable to outside.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 weight 500
```

35.82 network (BGP)

Command: network <*ip-address/M*> [route-map <*WORD*>] [backdoor]

no network <*ip-address/M*> [route-map <*WORD*>] [backdoor]

Function: Configure the BGP managed network, the route map specified in network application, or set the "back door" for the network. The "**no network <*ip-address/M*> [route-map <*WORD*>] [backdoor]**" command cancels this configuration.

Parameter: <*ip-address/M*>: Network prefix identifier

<*WORD*>: Name of route-map

Default: None

Command Mode: BGP route mode

Usage Guide: As for BGP routes, specify the route through which the BGP advertisements go. With the network defined by this command, the peer will be spreaded into the route map of the neighbor even if there is no route locally. Using the attribute specified in the network application through route map, when specifying the route comes from EBGP or inside the network through back door parameters, the inside route will be the optimized route even if the external route is of shorter distance.

Example:

```
Switch(config-router)# network 172.16.0.0/16
```

35.83 redistribute (BGP)

Command: redistribute <*ROUTES*> [route-map <*WORD*>]

no redistribute <*ROUTES*> [route-map <*WORD*>]

Function: Set the BGP to redistribute route from other modes into BGP. The "**no redistribute <*ROUTES*> [route-map <*WORD*>]**" command cancels this configuration.

Parameter: <*ROUTES*>: Route source or protocol, including: connected, ISIS, kernel, OSPF, RIP, static, etc.

<*WORD*>: Name of route map.

Default: None.

Command Mode: BGP Route Mode.

Usage Guide: Route from other ways will be distributed into the BGP route table with this command and transmitted to the neighbors.

Example: The static route is introduced into BGP with this configuration and advertised to the neighbors.

```
Switch(config-router)# redistribute static
```

35.84 redistribute ospf

Command: redistribute ospf [<*process-id*>] [route-map<*word*>]

no redistribute ospf [<*process-id*>]

Function: To redistribute routing information form OSPF to BGP. The no form of this command will remove the configuration.

Parameters: process-id is the process ID of the OSPF, limited between 1 and 65535. If no process id is specified, the default process id will be used.

route-map<*word*> is the pointer to the introduced routing map.

Default: Not redistributed by default.

Command Mode: BGP Configuration Mode.

Usage Guide: None.

Example: To redistribute routing of OSPF v2 to BGP (as number is 1).

```
Switch(config)#router bgp 1

Switch (config-router)#redistribute ospf 2
```

35.85 redistribute ospf (MBGP4+)

Command: redistribute ospf [<*process-tag*>] [route-map<*word*>]

no redistribute ospf [<*process-tag*>]

Function: To redistribute routing information form OSPFv3 to MBGP4+. The no form of this command will remove the configuration.

Parameters: process-id is the process character string of the OSPFv3, the length is less than 15. If no process id is specified, the default process will be used.

route-map<*word*> is the pointer to the introduced routing map.

Default: Not redistributed by default.

Command Mode: BGP IPv6 Configuration Mode.

Usage Guide: None.

Example: To redistribute routing information from OSPFv3 process with the tag as ABC to MBGP4+ (as number as 1).

```
Switch (config)#router bgp 1
```

Switch (config-router)#address-family ipv6 unicast
Switch (config-router-af)#redistribute ospf abc

35.86 rd

Command: rd <rd-val>

Function: Configure the VRF route identification label.

Parameter:*<rd-val>* is the route identification label, which normally should be（AS number or IP address）: digits, such as: 100:10

Command Mode: vrf mode

Usage Guide: Under VRF mode the configured RD is for identifying different VRF each of which shall have a unique RD; The BGP distinct routes with different VRF with this identification label. But attention should be paid on that once RD is configured, it will not be changed. So there is no form command to cancel this configuration and you have to reconfigure VRF

Example:

Switch(config)#ip vrf DC1
Switch(config-vrf)#rd 100:10
Switch(config-vrf)#

Above example creates a VRF named DC1 with RD value at 100:10

35.87 router bgp

Command: router bgp *<as-id>*

no router bgp *<as-id>*

Function: Enable BGP instance. The "**no router bgp *<as-id>***" command deletes BGP instance.

Parameter: *<as-id>*: 1-65535 is AS number.

Default: BGP not enabled.

Command Mode: Global mode

Usage Guide: Enable BGP by specified AS, and then enter the config-router state, the protocol can be configured at this prompt.

Example:

Switch(config)#router bgp 200
Switch(config-router)#exit

35.88 route-target

Command: route-target {import|export|both} <rt-val>

no route-target {import|export|both} *<rt-val>*

Function: Configure the route extended community attributes, so to determine whether the route be spreader to specific VRF.

Parameter:*<rt-val>* is the same as RD form, standing for the extended community attributes of the routes.

Command Mode: vrf mode

Usage Guide: Under VRF mode, the configured RT attributes decides which VRF will accept the route. There are 3 RT configurations: the import RT stands for the RT value acceptable by this VRF, the export RT represents the RT value carried with this VRF when routing spreading, both refers to above two option both enabled. If the export RT carried with the received route ever matches with the import RT of this VRF, then this VRF will accept this route or else not (except for the no bgp inbound-route-filter is configured which enables RD match). Several RT can be configured on the same VRF. Normally we set one RT with the both mode so to equal the RD and RT_VALUE.

Example:

```
Switch(config)#ip vrf DC1
Switch(config-vrf)#rd 100:10
Switch(config-vrf)#route-target both 100:10
Switch(config-vrf)#
```

In above example is created a VRF named DC1 with RD value 100:10. the RT is configured bilateral. The RT-VALUE is equal to RD.

35.89 set vpnv4 next-hop

Command: set vpnv4 next-hop <ip-addr>

no set vpnv4 next-hop *<ip-addr>*

Function: Configure the nexthop of the VPNv4 route.

Parameter: *<ip-addr>*is nexthop of vpnv4 route

Command Mode: vrf mode

Usage Guide: Configure VPNv4 route nexthop with this command. As normal nexthop settings are only for IPv4 route, this command specially configures the VPNv4 address-family.

Example:

Configure the address-family as follows:

```
Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
```

Switch(config-map)#set weight 655
Switch(config-map)#set vpnv4 next-hop 10.1.1.250
Switch(config-map)#exit
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.68 remote-as 100
Switch(config-router)#neighbor 10.1.1.68 route-map map1 in
Switch(config-router)#address-family vpnv4 unicast
Switch(config-router-af)#neighbor 10.1.1.68 activate
Switch(config-router-af)#exit-address-family View the routing message after refresh
Switch#show ip bgp vpn all Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 100:10 (Default for VRF DC1) *> 11.1.1.0/24 11.1.1.64 0 0 200 ? *>i15.1.1.0/24 10.1.1.250 0 100 655 200 ? *> 20.1.1.0/24 11.1.1.64 0 0 200 ? *>i100.1.1.0/24 10.1.1.250 0 100 655 200 ? Route Distinguisher: 100:10 *>i15.1.1.0/24 10.1.1.68 0 100 0 200 ? *>i100.1.1.0/24 10.1.1.68 0 100 0 200 ?

We can see that the nexthop 10.1.1.68 of the VPN route is changed to 10.1.1.250 after applied with route-ma

35.90 show ip bgp

Command: show ip bgp [<*ADDRESS-FAMILY*>] [<*ip-address*>|<*ip-address/M*> [longer-prefixes]| cidr-only]

Function: For displaying the routing messages permitted by BGP.

Parameter: <*ADDRESS-FAMILY*>: address-family such as “ipv4 unicast”

<*ip-address*>: IP address

<*ip-address/M*>: IP address and the mask

Default: None.

Command Mode: Admin and configuration mode

Usage Guide: We can display BGP routing messages by different parameters (such as address-family or IPv4 address), or a route covered by a prefix, or only the routing message don't match the earliest IP address-family (namely the route is not A or B or C type address.)

Example:

```
Switch#show ip bgp
BGP table version is 147, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 12.0.0.0         10.1.1.121               0             32768 ?
*> 100.1.1.0/24     10.1.1.200               0             32768 ?
*> 100.1.2.0/24     10.1.1.200               0             32768 ?
*> 172.0.0.0/8      0.0.0.0                                32768 i
Total number of prefixes 4
```

35.91 show ip bgp attribute-info

Command: show ip bgp attribute-info

Function: Display the BGP attributes messages.

Parameter: None.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: For displaying the attribute messages permitted by BGP.

Example:

```
Switch#sh ip bgp attribute-info
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.1.1.64
attr[3] nexthop 10.1.1.64
attr[1] nexthop 10.1.1.121
attr[2] nexthop 10.1.1.200
```

35.92 show ip bgp community

Command: show ip bgp [<*ADDRESS-FAMILY*>] community <*TYPE*> [exact-match]

Function: For displaying route permitted by BGP with community information.

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as "ipv4 unicast"

<*TYPE*>: Community attributes number show in AA:NN form or combination of local-AS, no-advertise, and no-export.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can choose several communities at a time, exact-match shows only the perfect match entries will be displayed.

Example:

```
Switch#show ip bgp community
BGP table version is 10, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
Total number of prefixes 2
```

35.93 show ip bgp community-info

Command: show ip bgp community-info

Function: For displaying the community messages permitted by BGP.

Parameter: None

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Messages in the same community multiply closable at the same time.

Example:

```
Switch#show ip bgp community-info
Address Refcnt Community
[0x3312558] (3) 100:50
```

35.94 show ip bgp community-list

Command: show ip bgp [<*ADDRESS-FAMILY*>] community-list <*NAME*> [exact-match]

Function: For displaying the routes containing the community list messages and permitted by BGP

Parameter: <*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”

<*NAME*>: Community list

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Configure the community list with ip community-list command and the contained community as well. When displayed with its name, communities included in all the lists are contained.

Example:

```
Switch(config)#ip community-list commu per 100:50
```

```
Switch#sh ip bgp community-list commu
BGP table version is 25, local router ID is 10.1.1.64
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
```

Related Command: ip community-list

35.95 show ip bgp dampening

Command: show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths>|<flap-statistics>|<parameters>}

Function: Display the routes permitted by BGP and relevant to the route dampening.

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Only the surged routes will be displayed. The Parameters shows the display configuration other than specific routes. The other two options will respectively show the restrained route and the dampening (recently recovered from invalid) routing messages.

Example:

```
Switch#sh ip bgp dampening dampened-paths
BGP table version is 12, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Reuse     Path
*d 100.1.3.0/24     10.1.1.64       00:27:40 100 ?

Total number of prefixes 1
```

```
Switch#sh ip bgp dampening flap-statistics
BGP table version is 13, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps  Duration  Reuse    Path
*d 100.1.3.0/24     10.1.1.64       3  00:06:05  00:27:00  100 ?
Switch#sh ip bgp dampening parameters
```

```
 dampening 15 750 2000 60 15 (route-map rmp)
   Reach ability Half-Life time       : 15 min
   Reuse penalty                      : 750
   Suppress penalty                   : 2000
   Max suppress time                  : 60 min
   Un-reach ability Half-Life time : 15 min
   Max penalty (ceil)                 : 11999
   Min penalty (floor)                : 375
Total number of prefixes 1
```

Related Command: bgp dampening

35.96 show ip bgp filter-list

Command: show ip bgp [<*ADDRESS-FAMILY*>] filter-list [<*WORD* >]

Function: For displaying the routes in BGP meeting the specific AS filter list.

Parameter: <*ADDRESS-FAMILY*>: address-family such as “ipv4 unicast”

< *WORD* >: AS-PATH access-list name

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Configure AS access-list with ip as-path access-list command. This command can show the routes passed the access-list.

Example:

```
Switch#SH IP BGP filter-list FL
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop                Metric LocPrf Weight Path
*> 100.1.1.0/24        10.1.1.64                    0                0 100 ?
Total number of prefixes 1
```

Related Command: neighbor filter-list, ip as-path access-list

35.97 show ip bgp inconsistent-as

Command: show ip bgp [<*ADDRESS-FAMILY*>] inconsistent-as

Function: For displaying routes with inconsistent BGP AS.

Parameter: <*ADDRESS-FAMILY*>: address family such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: If same prefix comes from different origin AS, the AS will be regarded as inconsistent. This command is for displaying this kind of routes.

Example:

```
Switch#sh ip bgp inconsistent-as
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.68                0             0 300 ?
*>                  10.1.1.64                0             0 100 ?
Total number of prefixes 1
```

35.98 show ip bgp neighbors

Command: show ip bgp [<*ADDRESS-FAMILY*>] neighbors [IP-ADDRESS] [advertised-routes|received {prefix-filter|routes}|routes]

Function: For displaying the BGP neighbor related messages.

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as “ipv4 unicast”

<*ip-address*>: Neighbor IP address

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display detailed messages of all neighbors by this command without parameters. Specifying IP address will show the detailed information of the neighbors with specified IP address. The advertised-routes、received prefix-filter、received routes、routes parameters will respectively displays the routes broadcast on local side, the received prefix filter, received routes (soft reconfiguration enabled) and the routing message from specific neighbor.

Example:

```
Switch#sh ip bgp neighbor
BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 11.1.1.100
  BGP state = Established, up for 00:13:43
  Last read 00:13:43, hold time is 240, keep alive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
```

```
For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes
Connections established 7; dropped 6
```

35.99 show ip bgp paths

Command: show ip bgp [<*ADDRESS-FAMILY*>] paths

Function: Display the path message permitted by BGP.

Parameter: <*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”.

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display the BGP path message includes the utilization state.

Example:

```
Switch#sh ip bgp paths
Address          Refcnt Path
[0x331dad0:0] (1)
[0x331d850:93] (1) 600
[0x331d8d8:249] (2) 200 300
```

35.100 show ip bgp prefix-list

Command: show ip bgp [<*ADDRESS-FAMILY*>] prefix-list [<*NAME*>]

Function: For displaying the route meet the specific prefix-list in BGP.

Parameter: <*ADDRESS-FAMILY*>: Address family such as “ipv4 unicast”

<*NAME*>: Name of prefix-list

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can select the required BGP route by regular expression.

Example:

```
Switch(config)#ip prefix-list PL permit any
```

```
Switch(config)#
```

```
Switch#sh ip bgp prefix-list PL
BGP table version is 1, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.66                              0 200 300 ?
*>                   10.1.1.100               0             32768 ?
Total number of prefixes 1
```

35.101 show ip bgp quote-regexp

Command: show ip bgp [<*ADDRESS-FAMILY*>] quote-regexp [<WORD>]

Function: For displaying the BGP route meets the specific AS related regular expression.

Parameter: <ADDRESS-FAMILY>: **>**: address-family such as “ipv4 unicast”

<WORD>: Regular expression

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Selecting the required route through regular expressions.

Example:

```
Switch#sh ip bgp quote-regexp ^300$
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.68               0             0 300 ?
Total number of prefixes 1
```

```
Switch#sh ip bgp quote-regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.64               0             0 500 100 600 ?
Total number of prefixes 1
```

35.102 show ip bgp regexp

Command: show ip bgp [<*ADDRESS-FAMILY*>] regexp [<*LINE*>]

Function: For displaying the BGP routes meets specific AS related normal expressions.

Parameter: <*ADDRESS-FAMILY*>: **>**: address-family such as “ipv4 unicast”

<*LINE*>: Regular expression

Default: None

Command Mode: Admin and configuration mode

Usage Guide: We can select BGP route of the required AS with normal expression.

Example:

```
Switch#sh ip bgp regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
Total number of prefixes 1
```

35.103 show ip bgp route-map

Command: show ip bgp [<*ADDRESS-FAMILY*>] route-map [<*NAME*>]

Function: For displaying the BGP routes meets the specific related route map.

Parameter: <*ADDRESS-FAMILY*>: such as “ipv4 unicast”

<*NAME*>: Name of route map

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Configure the route map with the route-map command, through which it can be displayed that process routes with route map. The command will display the routes meet specific route map.

Example:

```
Switch#sh ip bgp route-map rmp
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
*>                   10.1.1.68                0              0 300 ?
Total number of prefixes 1
```

35.104 show ip bgp scan

Command: show ip bgp scan

Function: For displaying BGP scan messages.

Parameter: None

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Scan regularly the nexthop messages. The command can show the current interval and related routes.

Example:

```
Switch#show ip bgp scan
BGP Instance: (Default) AS 200, router-id 11.1.1.100
BGP scan interval is 60
Current BGP nexthop cache:
```

Related Command: bgp scan-time

35.105 show ip bgp summary

Command: show ip bgp [<*ADDRESS-FAMILY*>] summary

Function: For displaying the BGP summary information.

Parameter: <*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”.

Default: None.

Command Mode: Admin and configuration mode

Usage Guide: Display some basic summary information of BGP.

Example:

```
Switch#show ip bgp summary
BGP router identifier 10.1.1.66, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.68       4        300       0       0        0    0    0    never    Active
Total number of neighbors 1
```

Display Contents Explanation
identifier Local identifier
local AS number The number of AS of local router
table version the version number of BGP interior database
AS-PATH entries The tabulation of the AS-PATH entries

community entries The property of the community entries
Neighbor Neighbor address
V The BGP version of neighbor running
AS The AS number of neighbor what is affiliated with
MsgRcvd The amount of message received from neighbor
MsgSent The amount of message sent to the neighbor
TblVer the version of route table
Up/Down It will display the conversation time length if the state with neighbor was established, otherwise display the present status.
State/PfxRcd If the state is established, display the amount of the prefix received of the router.otherwise,display the state of the neighbor at present.

35.106 show ip bgp view

Command: show ip bgp view [<*NAME*>] [<*ip-address*> | <*ip-address/M*> | [<*ADDRESS-FAMILY*>] summary]

Function: For displaying the messages of specified BGP instance.

Parameter: <*NAME*>: Name of BGP instance

<*ip-address*>: IP address

<*ip-address/M*>: IP address and mask

<*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display messages of specified BGP instance.

Example:

```
Switch#show ip bgp view as300 100.1.1.0/24
```

Related Command: router bgp

35.107 show ip bgp view neighbors

Command: show ip bgp view [<*NAME*>] neighbors [<*ip-address*>]

Function: Display neighbor messages of specified BGP instance.

Parameter: <*NAME*>: Name of BGP instance

<*ip-address*>: neighbor IP address

Default: None

Command Mode: Admin and configuration mode

Usage Guide: Display neighbor messages of specified BGP instance.

Example:

```
Switch#show ip bgp view as300 neighbors
```

35.108 show ip bgp vpnv4

Command: show ip bgp vpnv4 {all|rd <rd-val>|vrf <vrf-name>}

Function: Display the BGP VPN routing messages

Parameter: ***<rd-val>*** is the route identification label which is normally the（AS number or IP address）: digits, such as 100:10; ***<vrf-name>*** is the name of VRF, created through if vrf <*vrf-name*> command

Command Mode: All modes

Usage Guide: Available to display by specified RD or VRF.

Example:

```
Switch#sh ip bgp vpn all
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF DC1)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
```

35.109 show ipv6 bgp redistribute

Command: show ipv6 bgp redistribute

Function: Show the configuration information of redistribution other out routing to MBGP4+.

Parameter: None.

Default: Not shown by default.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: None.

Example:

```
Switch#show ipv6 bgp redistribute
```

35.110 timers bgp

Command: timers bgp *<0-65535> <0-65535>*

no timers bgp [*<0-65535> <0-65535>*]

Function: Configure all neighbor time in BGP. The "**no timers bgp [*<0-65535> <0-65535>*]**" command restores these times to default value.

Parameter: *<0-65535>* Respectively the KEEPALIVE interval and the hold time.

Default: KEEPALIVE is 60s, HOLD TIME is 240s.

Command Mode: BGP route mode

Usage Guide: Similar to neighbor time configuration which just performed on all neighbors

Example:

```
Switch(config-router)# timers bgp 50 200
```

Relevant Commands: neighbor timers, no neighbor timers

Chapter 36 Commands for Black Hole Routing

36.1 ip route null0

Command: ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>|<*prefix-length*>} null0 [<*distance*>]

no ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>|<*prefix-length*>} null0

Function: To configure routing destined to the specified network to the interface of null0.

Parameters: <*ip-prefix*> and **<*mask*>** are the IP address and network address mask of the destination, in dotted decimal format: **<*ip-prefix*>** and **<*prefix-length*>** are the IP address of the destination and the length of the prefix respectively; **null0** is the output interface for the black hole routing; **<*distance*>** is the management distance of the routing entry with limitation between 1 and 255.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: Null0 should be used as the output interface for IPv4 Black Hole Routing.

Example: To configure the routing to 192.168.188.0/24 as a Black Hole Routing.

```
Switch (config)# ip route 192.168.188.0/24 null0 20
```

36.2 ipv6 route null0

Command: ipv6 route <*ipv6-prefix*|*prefix-length*> null0 [<*precedence*>]

no ipv6 route <*ipv6-prefix*|*prefix-length*> null0

Function: To configure routing destined to the specified network to the interface of null0.

Parameters: <*ipv6-prefix*> is the IPv6 network static route addressof the destination, in dotted decimal format. **<*prefix-length*>** is the IPv6 address of the destination and the length of the prefix. **null0** is the output interface for the black hole routing. **<*precedence*>** is the route weight, ranging between 1 to 255 and 1 by default.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: When configuring IPv6 Black Hole Routing, it is much like configuring normal static routing, but using null0 as the output interface.

Example:

```
To configure a route to 2001:2:3:4::/64 as a Black Hole Routing.
```

Chapter 37 Commands for ECMP

37.1 maximum-paths

Command: maximum-paths <1-32>

no maximum-paths

Function: This command is used to configure the maximum-paths which support the equivalence multi-paths. The no command restores the default configuration.

Parameter: <1-32>: At present, users can configure the multi-paths number from 1 to 32. When configure 1, it is equal to disable ECMP function. In addition, the actual configuration number is the power of 2 that approaches and is bigger than the user input value.

Command mode: Global Mode.

Default: The default number is 4.

Usage Guide: None.

Example: Configure the maximum-paths of the equivalence multi-paths as 8.

```
Switch(config)# maximum-paths 8
```

Chapter 38 IPv4 Multicast Protocol

38.1 Public Commands for Multicast

38.1.1 show ip mroute

Command: show ip mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv4 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr: show the multicast route entries relative to this source address.

Default: None

Command Mode: Admin mode and global mode

Usage Guide:

Example: show all entries of multicast route table.

```
Switch(config)#show ip mroute
Name: Loopback, Index: 2002, State:49
Name: null0, Index: 2003, State:49
Name: sit0, Index: 2004, State:80
Name: Vlan1, Index: 2005, State:1043
Name: Vlan2, Index: 2006, State:1002
Name: pimreg, Index: 2007, State:c1
The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0
Group           Origin          Iif             Wrong     Oif:TTL
225.1.1.1       192.168.1.136   vlan1           0         2006:1
```

Displayed information Explanation
Name the name of interface
Index the index number of interface
State the state of interface
The total matched ipmr active mfc entries The total matched active IP multicast route mfc （multicast forwarding cache） entries
unresolved ipmr entries unresolved ip multicast route entries

Group the destination address of the entries
Origin the source address of the entries
Iif ingress interface of the entries
Wrong packets received from the wrong interface
Oif egress interface of the entries
TTL the value of TTL

38.2 Commands for PIM-DM

38.2.1 debug pim timer sat

Command: debug pim timer sat

no debug pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug pim timer sat**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

```
Switch # debug ip pim timer sat
```

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM handbook.

38.2.2 debug pim timer srt

Command: debug pim timer srt

no debug pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug pim timer srt**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail.

Example:

```
Switch #debug ip pim timer srt
```

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM manual section.

38.2.3 ip mroute

Command: ip mroute *<A.B.C.D> <A.B.C.D> <ifname> <.ifname>*

no ip mroute *<A.B.C.D> <A.B.C.D>* [*<ifname> <.ifname>*]

Function: To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.

Parameter: ***<A.B.C.D> <A.B.C.D>*** are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Default: To delete this static multicast entry, if the command isn't included interface parameter.

Command Mode: Global Mode.

Usage Guide: The ***<ifname>*** should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example:

```
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30
```

38.2.4 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

```
Switch(Config-if-Vlan1)#no ip pim bsr-border
```

38.2.5 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ip pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None.

Default: Disable PIM-DM protocol.

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ip multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one swtich.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim dense-mode

38.2.6 ip pim dr-priority

Command: ip pim dr-priority *<priority>*

no ip pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: *<priority>* is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ip pim dr-priority 100
Switch (Config -if-Vlan1)#

38.2.7 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid
Switch (Config-if-Vlan1)#

38.2.8 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets,this value is to describe neighbore holdtime,if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ip pim hello-holdtime 10
Switch (Config -if-Vlan1)#

38.2.9 ip pim hello-interval

Command: ip pim hello-interval < *interval*>

no ip pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode.

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime.

Example: Configure PIM-DM hello interval on interface vlan1.

```
Switch (config)#interface vlan1
Switch(Config-if-Vlan1)#ip pim hello-interval 20
```

38.2.10 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

```
Switch (config)#ip pim multicast-routing
```

38.2.11 ip pim neighbor-filter

Command: ip pim neighbor-filter *<list-number>*

no ip pim neighbor-filter *<list-number>*

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: *<list-number>*: *<list-number>* is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure vlan's filtering rules of pim neighbors.

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2     4294967294 / DR
```

```
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#
```

38.2.12 ip pim scope-border

Command: ip pim scope-border [<*1-99* >|<*acl_name*>]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <*1-99* >: is the ACL number for the management border.

<*acl_name*>: is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

38.2.13 ip pim state-refresh origination-interval

Command: ip pim state-refresh origination-interval <*interval*>

no ip pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message. The "**no ip pim state-refresh origination-interval**" command restores default value.

Parameter: <*interval*> packet transmission interval value is from 4s to 100s.

Default: 60s

Command Mode: Global Mode

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.

Example: Configure transmission interval of state-refresh message to 90s.

```
Switch (config)#ip pim state-refresh origination-interval 90
```

38.2.14 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example:

```
Switch(config)#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR     DR
                                    Mode   Count  Prior
10.1.4.3         Vlan1     0        v2/S   1      1      10.1.4.3
10.1.7.1         Vlan2     2        v2/S   0      1      10.1.7.1
```

Displayed Information Explanations
Address Interface address
Interface Interface name
VIF index Interface index
Ver/Mode Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count The interface's neighbor count
DR Prior Dr priority
DR The interface's DR address

38.2.15 show ip pim mroute dense-mode

Command: show ip pim mroute dense-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display PIM-DM message forwarding items.

Parameter: group <A.B.C.D>: displays forwarding items relevant to this multicast address.

source <A.B.C.D>: displays forwarding items relevant to this source.

Default: Do not display (Off).

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

```
Switch(config)#show ip pim mroute dense-mode
IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, 226.0.0.1)
  Local        ..l.....................

(192.168.1.12, 226.0.0.1)
RPF nbr: 0.0.0.0
RPF idx: Vlan2
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local        .....................
  Pruned       .....................
  Asserted     .....................
  Outgoing     ..o.....................
```

```
Switch#
```

Displayed Information Explanations
(*,226.0.0.1) (*,G) Forwaridng item
(192.168.1.12, 226.0.0.1) (S,G) Forwarding item
RPF nbr Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx

Interface located in RPF neighbor
Upstream State Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local Local position joins interface, the interface receives IGMP Join
Pruned PIM prunes interface, the interface receives Prune messages
Asserted Asserted state
Outgoing Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

38.2.16 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

```
Switch (config)#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                      Priority/Mode
```

```
10.1.6.1        Vlan1        00:00:10/00:01:35 v2    1 /
10.1.6.2        Vlan1        00:00:13/00:01:32 v2    1 /
10.1.4.2        Vlan3        00:00:18/00:01:30 v2    1 /
10.1.4.3        Vlan3        00:00:17/00:01:29 v2    1 /
```

Displayed Information Explanations
Neighbor Address Neighbor address
Interface Neighbor interface
Uptime/Expires Running time /overtime
Ver Pim version ,v2 usually
DR Priority/Mode DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

38.2.17 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

```
Switch(config)#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination      Type  Nexthop  Nexthop          Nexthop    Nexthop  Metric  Pref   Refcnt
Num      Addr             Ifindex  Name
192.168.1.1      N...  1        0.0.0.0          2006               0       0      1
192.168.1.9      ..S.  1        0.0.0.0          2006               0       0      1
```

Displayed Information Explanations
Destination Destination of next item
Type N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num Nexthop number
Nexthop Addr Nexthop address
Nexthop Ifindex Nexthop interface index
Nexthop Name Nexthop name
Metric Metric Metric to nexthop
Pref Preference Route preference
Refcnt Reference count

38.3 Commands for PIM-SM

38.3.1 clear ip pim bsr rp-set

Command: clear ip pim bsr rp-set *

Function: Clear all RP.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Clear all RP rapidly.

Example: Clear all RP.

```
Switch# clear ip pim bsr rp-set *
```

Relative Command: show ip pim bsr-router

38.3.2 debug pim event

Command: debug pim event

no debug pim event

Function: Enable or Disable pim event debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim event debug switch and display events information about pim operation.

Example:

Switch#

```
Switch# debug ip pim event
Switch#
```

38.3.3 debug pim mfc

Command: debug pim mfc

no debug pim mfc

Function: Enable or Disable pim mfc debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.

Example:

```
Switch# debug ip pim mfc
```

38.3.4 debug pim mib

Command: debug pim mib

no debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example:

```
Switch# debug ip pim mib
```

38.3.5 debug pim nexthop

Command: debug pim nexthop

no debug pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example:

```
Switch# debug ip pim nexthop
```

38.3.6 debug pim nsm

Command: debug pim nsm

no debug pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example:

```
Switch# debug ip pim nsm
```

38.3.7 debug pim packet

Command: debug pim packet

debug pim packet in

debug pim packet out

no debug pim packet

no debug pim packet in

no debug pim packet out

Function: Enable or Disable pim debug switch

Parameter: in display only received pim packets

out display only transmitted pim packets

none display both

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the received and transmitted pim packets by this switch.

Example:

```
Switch# debug ip pim packet in
```

38.3.8 debug pim state

Command: debug pim state

no debug pim state

Function: Enable or Disable pim debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the changing information about pim state by this switch.

Example:

```
Switch# debug ip pim state
```

38.3.9 debug pim timer

Command: debug pim timer

debug pim timer assert

debug pim timer assert at

debug pim timer bsr bst

debug pim timer bsr crp

debug pim timer bsr

debug pim timer hello ht

debug pim timer hello nlt

debug pim timer hello tht

debug pim timer hello

debug pim timer joinprune et

debug pim timer joinprune jt

debug pim timer joinprune kat

debug pim timer joinprune ot

debug pim timer joinprune plt

debug pim timer joinprune ppt

debug pim timer joinprune pt

debug pim timer joinprune

debug pim timer register rst

debug pim timer register

no debug pim timer

no debug pim timer assert

no debug pim timer assert at

no debug pim timer bsr bst

no debug pim timer bsr crp

no debug pim timer bsr

no debug pim timer hello ht

no debug pim timer hello nlt

no debug pim timer hello tht

no debug pim timer hello

no debug pim timer joinprune et

no debug pim timer joinprune jt

no debug pim timer joinprune kat

no debug pim timer joinprune ot

no debug pim timer joinprune plt

no debug pim timer joinprune ppt

no debug pim timer joinprune pt

no debug pim timer joinprune

no debug pim timer register rst

no debug pim timer register

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable the specified timer's debug information.

Example:

```
Switch# debug pim timer assert
```

38.3.10 ip mroute

Command: ip mroute *<A.B.C.D> <A.B.C.D> <ifname> <.ifname>*

no ip mroute *<A.B.C.D> <A.B.C.D>* [*<ifname> <.ifname>*]

Function: To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.

Parameter: *<A.B.C.D> <A.B.C.D>* are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Default: To delete this static multicast entry, if the command isn't included interface parameter.

Command Mode: Global Mode.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example:

```
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30
```

38.3.11 ip pim accept-register

Command: ip pim accept-register list *<list-number>*

no ip pim accept-register

Function: Filter the specified multicast group and multicast address.

Parameter: <***list-number***>: ***<list-number>*** is the access-list number ,it ranges from 100 to 199.

Default: Permit the multicast registers from any sources to any groups.

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured ,the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

```
Switch(config)#ip pim accept-register list 120
Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10    0.0.0.255
Switch (config)#
```

38.3.12 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

```
Switch(Config-if-Vlan1)#no ip pim bsr-border
```

38.3.13 ip pim bsr-candidate

Command: ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>} [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command **"no ip pim bsr-candidate"** disables the candidate BSR.

Parameter: ***Ifname*** is the specified interface's name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured ,the default priority value is 0.

Default: This switch is not a candidate BSR router.

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to

configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured , this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

```
Switch (config)# ip pim bsr-candidate vlan1 30 10
```

38.3.14 ip pim cisco-register-checksum

Command: ip pim cisco-register-checksum [group-list <*simple-acl*>]

no ip pim cisco-register-checksum [group-list <*simple-acl*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the register packet's head length, default: 8

Parameter: <*simple-acl*>: <1-99> Simple access-list **<*simple-acl*>:** <1-99> Simple access-list

Command Mode: Global Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

```
Switch (config)#ip pim cisco-register-checksum group-list 23
```

38.3.15 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

```
Switch (config)# interface vlan 1
```

```
Switch(Config-if-Vlan1)ip pim dr-priority 100
```

```
Switch (Config -if-Vlan1)#
```

38.3.16 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no**

ipv6 pim exclude-genid" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid
Switch (Config-if-Vlan1)#

38.3.17 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime,if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Hold time's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ip pim hello-holdtime 10
Switch (Config -if-Vlan1)#

38.3.18 ip pim hello-interval

Command: ip pim hello-interval <*interval*>

no ip pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ip pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime.

Example: Configure vlan's pim-sm hello interval

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim hello-interval 20
Switch(Config-if-Vlan1)#
```

38.3.19 ip pim ignore-rp-set-priority

Command: ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configure the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: Disabled

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example:

```
Switch (config)#ip pim ignore-rp-set-priority
```

38.3.20 ip pim jp-timer

Command: ip pim jp-timer <*value*>

no ip pim jp-timer

Function: Configure to add JP timer. the "**no ip pim jp-timer**" command restores the default value.

Parameter: **<*value*>** ranges from 10 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of JOIN-PRUNE packets sent by PIM periodically, the default value is 60s. The default value is recommended if no special reasons.

Example: Configure the interval of timer

```
Switch (config)#ip pim jp-timer 59
```

38.3.21 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (config)#ip pim multicast-routing
Switch (config)#

38.3.22 ip pim neighbor-filter

Command: ip pim neighbor-filter *<list-number>*

no ip pim neighbor-filter *<list-number>*

Function: Configure the neighbor access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: *<list-number>*: *<list-number>* is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any.

Example: Configure vlan's filtering rules of pim neighbors.

Switch #show ip pim neighbor Neighbor Address Interface Uptime/Expires Ver DR Priority/Mode 10.1.4.10 Vlan1 02:30:30/00:01:41 v2 4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any
Switch (config)#show ip pim neighbor

38.3.23 ip pim register-rate-limit

Command: ip pim register-rate-limit <*limit*>

no ip pim register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets; the unit is packet/second. The "**no ip pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's ,not the whole system's.

Parameter: <*limit*> ranges from 1 to 65535.

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: This configuration is to prevent the attack to DR, limiting sending REGISTER packets.

Example: Configure the speedrate of DR sending register packets to 59 p/s.

```
Switch (config)#ip pim register-rate-limit 59
```

38.3.24 ip pim register-rp-reachability

Command: ip pim register-rp-reachability

no ip pim register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration.

Parameter: None

Default: Do not check

Command Mode: Global Mode

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure DR to check the RP reachability.

```
Switch (config)#ip pim register-rp-reachability
```

```
Switch (config)#
```

38.3.25 ip pim register-source

Command: ip pim register-source {<*A.B.C.D*> | <*ifname*>| vlan <*vlan-id*>}

no ip pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter: <*ifname*> is the interface name,

<*vlan-id*> is VLAN ID;

<*A.B.C.D*> is the configured source IP addresses.

Default: Do not check

Command Mode: Global Mode

Usage Guide: The "**no ip pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address sent by DR.

```
Switch (config)#ip pim register-source 10.1.1.1
```

38.3.26 ip pim register-suppression

Command: ip pim register-suppression <*value*>

no ip pim register-suppression

Function: This command is to configure the value of register suppression timer, the unit is second. The "**no ip pim register-suppression**" command restores the default value.

Parameter: <*value*> is the timer's value, it ranges from 10 to 65535s.

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR, it's the value of register suppression timer; The bigger one of the default register keep-alive time of RP (210s) and the sum of triple register suppression time and 5. If configure this value on RP without the command "ip pim rp-register-kat", this command may modify the RP register keep-alive time.

Example: Configure the value of register suppression timer to 10s.

```
Switch (config)#ip pim register- suppression 10
```

38.3.27 ip pim rp-address

Command: ip pim rp- address <*A.B.C.D*> <*A.B.C.D/M*>

no ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]

Function: This command is to configure static RP globally or in a multicast address range.The **"no ipv6 pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]**" command cancels static RP.

Parameter: <*A.B.C.D*> is the RP address

<*A.B.C.D/M*> the scope of the specified RP address

<*all*> is all the range

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range and configure PIM-SM static RP information. Attention, when computing rp, BSR RP is selected first. If it doesn't succeed, static RP is selected.

Example: Configure vlan1 as candidate RP announcing sending interface globally.

```
Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8
```

38.3.28 ip pim rp-candidate

Command: ip pim rp-candidate { vlan < *vlan-id* > | <*ifname*>} [<*A.B.C.D/M*>] [<priority>]

no ip pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ip pim rp-candiate**" command cancels the candidate RP.

Parameter: ***vlan-id*** isVlan ID;

ifname is the name of the specified interface;

A.B.C.D/M is the ip prefix and mask;

<priority> is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority.

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured, this switch is the RP candidate router.

Example: Configure vlan1 as the sending interface of candidate RP announcing sending messages

```
Switch (config)# ip pim rp-candidate vlan1 100
```

38.3.29 ip pim rp-register-kat

Command: ip pim rp-register-kat <*vaule*>

no ip pim rp-register-kat

Function: This command is to configure the KAT（KeepAlive Timer）value of the RP（S, G）items, the unit is second. The "**no ip pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value, it ranges from 1 to 65535s.

Default: 185s

Command Mode: Global Mode

Usage Guide: This command is to configure the RP's keep alive time, during the keep alive time RP's（S,G）item will not be deleted because it hasn't received REGISTER packets. If no new REGISTER packet is received when the keep alive time is over, this item will be obsolete.

Example: Configure the kat value of RP's (S,G) item to 180s

```
Switch (config)#ip pim rp-register- kat 180
```

```
Switch (config)#
```

38.3.30 ip pim scope-border

Command: ip pim scope-border [<*1-99* >|<*acl_name*>]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <*1-99* >: is the ACL number for the management border.

***<acl_name>*:** is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

38.3.31 ip pim sparse-mode

Command: ip pim sparse-mode [passive]

no ip pim sparse-mode [passive]

Function: Enable PIM-SM on the interface; the "**no ip pim sparse-mode [passive]**" command disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP(reveice and transmit IGMP packets).

Default: Do not enable PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface.

Example: Enable PIM-SM on the interface vlan1.

```
Switch (config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip pim sparse-mode
```

```
Switch(Config-if-Vlan1)#
```

38.3.32 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode.

Usage Guide: Display the BSR information maintained by the PIM.

Example: show ip pim bsr-router

```
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 10.1.4.3 (?)
  Uptime:      00:06:07, BSR Priority: 0, Hash mask length: 10
  Next bootstrap message in 00:00:00
  Role: Candidate BSR
  State: Elected BSR
Next Cand_RP_advertisement in 00:00:58
  RP: 10.1.4.3(Vlan1)
```

Displayed Information Explanations
BSR address Bsr-router Address
Priority Bsr-router Priority
Hash mask length Bsr-router hash mask length
State The current state of this candidate BSR, Elected BSR is selected BSR

38.3.33 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example:

```
testS2(config)#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR     DR
                                    Mode   Count  Prior
10.1.4.3         Vlan1     0        v2/S   1      1      10.1.4.3
10.1.7.1         Vlan2     2        v2/S   0      1      10.1.7.1
```

Displayed Information Explanations
Address Interface address
Interface Interface name
VIF index Interface index

Ver/Mode Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count The interface's neighbor count
DR Prior Dr priority
DR The interface's DR address

38.3.34 show ip pim mroute sparse-mode

Command: show ip pim mroute sparse-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display the multicast route table of PIM-SM.

Parameter: group <A.B.C.D>: Display redistributed items that related to this multicast address

source <A.B.C.D>: Display redistributed items that related to this source

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example:

```
Switch #show ip pim mroute sparse-mode
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0

(*, 239.192.1.10)
RP: 10.1.6.1
RPF nbr: 10.1.4.10
RPF idx: Vlan1
Upstream State: JOINED
  Local       ..l.....................
  Joined      .....................
  Asserted    .....................
  Outgoing    ..o.....................
```

Displayed Information Explanations
Entries The counts of each item
RP Share tree's RP address
RPF nbr RP direction or upneighbor of source direction.
RPF idx RPF nbr interface
Upstream State Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local Local join interface, this interface receive IGMPJoin
Joined PIM join interface, this interface receive J/P messages
Asserted Asserted state
Outgoing Final outgoing of multicast data, in this example, the index of the outgoing interface is 2. Command "show ip pim interface" can query interface information.

38.3.35 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

```
Switch (config)#show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.6.1          Vlan1              00:00:10/00:01:35 v2      1 /
10.1.6.2          Vlan1              00:00:13/00:01:32 v2      1 /
10.1.4.2          Vlan3              00:00:18/00:01:30 v2      1 /
10.1.4.3          Vlan3              00:00:17/00:01:29 v2      1 /
```

Displayed Information Explanations
Neighbor Address Neighbor address
Interface Neighbor interface
Uptime/Expires Running time /overtime
Ver Pim version ,v2 usually
DR Priority/Mode DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

38.3.36 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

```
Switch(config)#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination      Type  Nexthop  Nexthop        Nexthop    Nexthop Metric Pref  Refcnt
                       Num      Addr           Ifindex    Name
____
192.168.1.1      N...  1        0.0.0.0        2006                0      0     1

192.168.1.9      ..S.  1        0.0.0.0        2006                0      0     1
```

Displayed Information Explanations
Destination Destination of next item
Type N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num Nexthop number
Nexthop Addr Nexthop address
Nexthop Ifindex Nexthop interface index
Nexthop Name Nexthop name
Metric Metric Metric to nexthop
Pref Preference Route preference
Refcnt Reference count

38.3.37 show ip pim rp-hash

Command: show ip pim rp-hash <*A.B.C.D*>

Function: Display the RP address of A,B,C,D's merge point

Parameter: Group address

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example:

```
Switch (Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10
      RP: 10.1.6.1
Info source: 10.1.6.1, via bootstrap
```

Displayed Information Explanations
RP Queried group'sRP
Info source The source of Bootstrap information

38.3.38 show ip pim rp mapping

Command: show ip pim rp mapping

Function: Display Group-to-RP Mapping and RP.

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the current RP and mapping relationship.

Example:

```
Switch (Config-if-Vlan1)#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
   RP: 10.1.6.1
      Info source: 10.1.6.1, via bootstrap, priority 6
            Uptime: 00:11:04
```

Displayed Information Explanations

Group(s) Group address range of RP
Info source Source of Bootstrap messages
Priority Priority of Bootstrap messages

38.4 Commands for MSDP Configuration

38.4.1 cache-sa-holdtime

Command: cache-sa-holdtime <*150-3600*>

no cache-sa-holdtime

Function: To configure the longest holdtime of SA table within MSDP Cache.

Parameter : *seconds* : the units are seconds, range between 150 to 3600.

Command Mode: MSDP Configuration Mode.

Default: 150 seconds by default.

Usage Guide: To configure the aging time of (S, G) table for MSDP cache as requirement.

Example:

Switch(router-msdp)#cache-sa-holdtime 350

Switch(config)#router msdp
Switch(router-msdp)#cache-sa-holdtime 350

38.4.2 cache-sa-maximum

Command: cache-sa-maximum <*sa-limit*>

no cache-sa-maximum

Function: To configure the maximum sa-limit of MSDP Peer cache specified.

Parameter: <*sa-limit*>: The maximum cache SA number，range between 1 to 75000.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: The maximum of cache SA number is 20000 by default.

Usage Guide: This command can be used to configure the maximum number of cached SA messages on the router in order to prevent the DoS – Deny of Service attack. The maximum number of cached SA messages can be configured in global configuration mode or in the MSDP Peer configuration mode. If the configured value is less than the current number of cached SA messages, or the number configured in global mode is less than that configured in peer mode, the configuration will not function.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#cache-sa-maximum50000
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# cache-sa-maximum 22000
```

38.4.3 cache-sa-state

Command: cache-sa-state

no cache-sa-state

Function: To configure the SA cache state of route.

Parameter: None.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: Enabled.

Usage Guide: To configure the SA cache state. If configured, the new groups will be able to get information about all the active sources from the SA cache and join the related source tree without having to wait for new SA messages. SA-cache should be enabled on all the MSDP speakers. The no form of this command will remove the configuration of SA cache. To be mentioned, this command should be issued exclusively with the sa-request command.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#no cache-sa-state
```

38.4.4 clear msdp peer

Command: clear msdp peer {*peer-address*| *}

Function: Disconnected between specified MSDP Peer and TCP, to clear the statistics of the Peer.

Parameter: *peer-address*: The IP address of the Peer;

***** Disconnected with all the Peers.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If this command is issued with peer-address, the TCP connection to the specified MSDP Peer will be removed. And all the statistics about the peer will be cleared. If no peer-address is appended, all the MSDP connections as long as relative statistics about peers will be removed.

Example:

```
Switch#clear msdp peer *
```

38.4.5 clear msdp sa-cache

Command: clear msdp sa-cache {group A.B.C.D|* }

Function: To clear the Source Active information in MSDP cache: the correspond data with all the sources from specified group, or the correspond data with one specified (S, G) item.

Parameter: *group-address :*The IP address of multicast group, to clear group (S, G) in the Cache.

***:** To clear all the items in the cache.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If group is specified, the non-local SA entries of the MSDP cache of the specified group. If no parameters are appended, all the non-local SA entries in the MSDP cache will be removed.

Example:

```
Switch#clear msdp sa-cache group 224.1.1.1
```

38.4.6 clear msdp statistics

Command: clear msdp statistics {*peer-address*| *}

Function: To clear MSDP statistic information, and not reset the session of MSDP Peer.

Parameter: *peer-address*: The IP address of Peer.

***** Disconnection with all the Peers.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

```
Switch#clear msdp statistics *
```

38.4.7 connect-source

Command: connect-source <*interface-type <interface-number>*

no connect-source <*interface-type> <interface-number>*

Function: To configure the interface address, which used for all the MSDP Peers to set up correspond connection between MSDP Peer and MSDP.

Parameter: <*interface-type> <interface-number*>: Interface type and interface number.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: There is no specified interface by default.

Usage Guide: The router use the IP address of this port to set up MSDP Peer connection with MSDP Peer. Pay attention: specified connect-source address must consitant with the configuration of Peer address, otherwise can not set up TCP connection. The configuration under MSDP Peer mode will cover with MSDP Mode. No command will cancel the configuration and set again all the MSDP connection of this port.

Example:

```
Switch(config)#router msdp
```

```
Switch(router-msdp)#connect-source interface vlan 2
```

```
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# connect-source interface loopback 10
```

38.4.8 debug msdp all

Command: debug msdp all

no debug msdp all

Function: To enable all the debugging information about MSDP; the no command disable all the debugging information.

Command Mode: Admin Configuration Mode.

Default: Disabled.

Usage Guide: Enable the debugging switch of MSDP, display the protocol packet send/receive information of MSDP Peer---packet, keepalive packet send/receive information---keepalive, event information---event, NSM mutual information---nsm, timer information---timer, protocol state information---fsm, filter policy information---filter.

Exampe:

```
Switch#debug msdp all
```

38.4.9 debug msdp events

Command: debug msdp events

no debug msdp events

Function: Enable /disable the switch of **msdp events debug**.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The event of running MSDP protocol can be monitored after enable this switch.

Example:

```
Switch#debug msdp events
```

38.4.10 debug msdp filter

Command: debug msdp filter

no debug msdp filter

Function: Enable/disable debug switch of MSDP filter policy information.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The filter information of MSDP receiving/sending message can be monitored after enable this switch.

Example:

```
Switch#debug msdp filter
```

38.4.11 debug msdp fsm

Command: debug msdp fsm

no debug msdp fsm

Function: Enable/disable debug switch of MSDP fsm.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: Enable this switch, the fsm information of MSDP Peer will be displayed.

Example:

```
Switch#debug msdp fsm
```

38.4.12 debug msdp keepalive

Command: debug msdp keepalive

no debug msdp keepalive

Function: Enable/disable the debug switch of keepalive message information for MSDP protocol.

Parameter: None.

Default: close the switch.

Command Mode: Admin Mode.

Usage Guide: The information of receiving/sending keepalive message for MSDP protocol can be monitored after enables this switch.

Example:

```
Switch#debug msdp keepalive
```

38.4.13 debug msdp nsm

Command: debug msdp nsm

no debug msdp nsm

Function: Enable/disable the switch of **msdp nsm debug**.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The alternation information between running MSDP protocol and NSM module can be monitored after enable this switch.

Example:

```
Switch#debug msdp nsm
```

38.4.14 debug msdp packet

Command: debug msdp packet {send | receive}

no debug msdp packet {send | receive}

Function: Enable/disable the debug switch of sending/receiving message for the MSDP protocol.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The receiving/sending messages of MSDP protocol can be monitored after enable this switch.

Example:

```
Switch#debug msdp packet send
```

38.4.15 debug msdp peer

Command: debug msdp peer A.B.C.D

no debug msdp peer

Function: Enable/disable all the debug information switch of specified MSDP Peer.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: Enable all the debug information of specified MSDP Peer as requirement, the debug information of other MSDP Peers will not be displayed. This command is take effect only for the specified last one MSDP peer.

Example:

```
Switch#debug msdp peer 10.1.1.1
```

38.4.16 debug msdp timer

Command: debug msdp timer

no debug msdp timer

Function: Enable/disable the debug switch of MSDP timer.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage guide: Enable dubug information for the specified timer as requirement.

Example:

```
Switch#debug msdp timer
```

38.4.17 default-rpf-peer

Command: default-rpf-peer <peer-address> [rp-policy <acl-list-number>|<word>]

no default-rpf-peer

Function: To configure static RPF peer.

Parameter: <peer-address>: the IP address of the MSDP peer.

<acl-list-number>: the ACL number, only support standard ACL from 1 to 99.

<word>: the standard ACL name.

Command Mode: MSDP Configuration Mode.

Default: There is no static RPF peer by default. If the peer command only configures one MSDP peer, this peer will be treated as the default peer.

Usage Guide: To configure more than one static RPF peers, make sure to use the following two configuration methods:

Both use the rp-policy parameter: multiple RPFs take effect at the same time, and filter RP in SA messages according to the configured prefix list, and only accept SA messages allowed to pass.

Neither uses the rp-policy parameter: according to the sequence of configuration, only the first static RPF peer in the state of UP is active. All SA messages from this peer can be received while those from other peers will be dropped. If the active peer loses effect (such as the configuration is canceled or the connection is disconnected), still choose the first static RPF peer in the state of UP in the configuration sequence to be the active static RPF peer.

Example:

Switch(config)#router msdp
Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

38.4.18 description

Command: description <*text*>

no description

Function: Add description information of specified MSDP Peer.

Parameter: *text*: Description text, range between 1 to 80 bytes.

Command Mode: MSDP Peer Configuration Mode.

Default: There is no specified by default.

Usage Guide: To add description for the specified MSDP Peer in order to identify the different MSDP configuration. The no form of this command will remove the description.

Example:

Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# description PLANET-20

38.4.19 exit-peer-mode

Command: exit-peer-mode

Function: Quit MSDP Peer configuration mode, and enter MSDP configuration mode.

Command Mode: MSDP Peer Configuration Mode.

Default: None.

Usage Guide: MSDP configuration mode can be returned to with the exit-peer-mode command, when configuration to an MSDP Peer is done.

Example: Back to MSDP configuration mode from MSDP Peer configuration mode.

```
Switch(config-msdp-peer)# exit-peer-mode
```

38.4.20 mesh-group

Command: mesh-group <*name*>

no mesh-group <*name*>

Function: To configure MSDP Peer as specified mesh group number, if set the same MSDP Peer to many mesh groups, then the last mesh group is available.

Parameter: name: Mesh-group name.

Command Mode: MSDP Peer Configuration Mode.

Default: MSDP Peer doesn't belong to any mesh group by default.

Usage Guide: Mesh group can reduce SA message flooding and predigest Peer-RPF checking.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# mesh-group PLANET-1
```

38.4.21 originating-rp

Command: originating-rp <*interface-type*> <*interface-number*>

no originating-rp

Function: Configure Originating RP address that to configure the IP address of the specified interface as the IP address of the RP in the SA messages.

Parameter: <*interface-type*> < *interface-number*>: type and number of the port.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: The default RP address of SA message is the RP address of PIM configured.

Usage Guide: To configure the IP address of the specified interface as the IP address of the RP in the SA messages. If no IP address is configured for the specified interface, or the interface is down, no SA messages will be advertised. In this occasion, if multiple RP is configured for the device, other SA messages for other RP will not be advertised either. Hence, it is required that the interface should be working when being configured.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#originating-rp vlan 20
```

38.4.22 peer

Command: peer <*A.B.C.D*>

no peer <*A.B.C.D*>

Function: To configure MSDP Peer, enter MSDP Peer mode; the no form command delete the configured MSDP Peer.

Command Mode: MSDP Configuration Mode.

Default: There is no MSDP Peer configured by default.

Usage Guide: To configure the IP address of the MSDP Peer, and enter the peer configuration mode. When the command is issued, the router will setup the TCP session to the specified peer. The no form of this command will remove the configured MSDP Peer, and destroy all the sessions and related statistics with the specified peer. Pay attention: specified Peer address must be corresponded with the interface address. If configure the Connect-source, the Peer address must be Connect-source interface address; if not specified Connect-source, the Peer address is the egress address, otherwise cannot set up TCP connection.

Example: To configure MSDP Peer in MSDP congfiguration mode.

```
Switch(config-msdp)#peer 10.1.1.1
Switch(config-msdp-peer)#
```

38.4.23 redistribute

Command: redistribute [list <*acl-list-number* | *acl-name*>]

no redistribute

Function: To configure the redistribute of SA messages.

Parameter: *acl-number*: specified advanced ACL number（100-199）.

acl-name: specified ACL name.

Command Mode: MSDP Configuration Mode.

Default: When set up SA message, announce all the source within fired, but not confine the (S, G) item.

Usage Guide: If ACL list number is specified, only the (S, G) entries which have passed the ACL check will be advertised in the SA messages. If no ACL is specified, no (S, G) entry will be advertised in the SA messages.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#redistribute list 130
```

38.4.24 remote-as

Command: remote-as <*as-num*>

no remote-as <*as-num*>

Function: To configure AS number of specified MSDP Peer.

Parameter: *as –num*: AS number, range between 1 to 65535.

Command Mode: MSDP Peer Configuration Mode.

Default: The AS number isn't initialized to 0 by default.

Usage Guide: This command set the AS number for specified Peer. The no command restores the AS number of specified MSDP Peer.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# remote-as 20
```

38.4.25 router msdp

Command: router msdp

no router msdp

Function: Enable the MSDP protocol of the switch, enter MSDP mode; the no form command disable MSDP protocol.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: Enable MSDP on global mode, but even configured PIM SM at the same time, then the MSDP can be work.

Example: Enable MSDP on global mode.

```
Switch(config)#router msdp
```

38.4.26 sa-filter

Command: sa-filter {**in | out**} [**list <*acl-number* | *acl-name*> | rp-list <*rp-acl-number* | *rp-acl-name*>]**

no sa-filter {**in | out**} [**list <*acl-number*| *acl-name*> | rp-list <*rp-acl-number* | *rp-acl-name*>]**

Function: To configure the filter policy of receiving or transmitting messages, which can be used to controls the receiving and transmitting source message.

Parameter: in: To filter the SA messages from specified MSDP Peer.

out: To filter the SA messages transmitted from specified MSDP Peer.

***acl-number*:** Specified advanced ACL number（100-199）.

***acl-name*:** Specified advanced ACL name.

***rp-acl-number*:** Specified standard ACL number（1-99）.

rp-*acl-name*: Specified standard ACL name.

If the parameter isn't specified, all the SA messages which include (S, G) item will be filtered.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: All the SA messages receiving or transmitting will not be filtered.

Usage Guide: Configuration in the peer mode will override that in the MSDP configuration mode. The distribution of SA messages can be controlled through this command or the redistribute command.

Example:

```
Switch(config)#router msdp
```

Switch(router-msdp)#sa-filter in
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# sa-filter in list 120

38.4.27 sa-request

Command: sa-request

no sa-request

Function: To configure the route sending SA request message to specified MSDP Peer when received the joined message from a new group.

Parameter: None.

Command Mode: MSDP Peer Configuration Mode.

Default: Not sending SA Request message by default.

Usage Guide: This command makes the switch (RP) send SA request messages to the specified MSDP. When there is a new group or member, the switch (RP) will send SA request messages to the specified MSDP and wait for the latter's response of its cached local SA messages. After sending a SA message to the specified MSDP, RP will receive a SA_response message from the peer, and know all active sources of the peer (not including the source information learnt via MSDP SA). If RP is configured with SA cache state, this configuration won't take effect. This command is mutually exclusive to sa-cache-sate. If the MSDP is configured with SA cache state, it won't be able to configure sa-request. The switch will show a prompt to notice the users. Please notice this command only applies to RP.

Example:

Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# sa-request

38.4.28 sa-request-filter

Command: sa-request-filter [list <*access-list-number* | *access-list-name*>]

no sa-request-filter [list <*access-list-number* | *access-list-name*>]

Function: All the SA request messages from MSDP Peer will be filtered.

Parameter: *access-list-number*: ACL number, only supported standard ACL from 1 to 99.

***access-list-name*:** ACL name.

Command Mode: MSDP Configuration Mode.

Default: The route receives all the SA request messages from MSDP Peer.

Usage Guide: If no list parameter is specified, all the SA request messages from MSDP Peers will be filtered. If specified, SA request messages will be filtered with the specified ACL list.

Example:

```
Switch(config)#router msdp
```

```
Switch(router-msdp)# sa-request-filter list 1
```

38.4.29 show msdp global

Command: show msdp global

Function: Show the configuration information in MSDP Mode.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information in MSDP mode, include the state of MSDP protocol, Cache and so on.

Example:

```
Switch#show msdp global
Multicast Source Discovery Protocol (MSDP):
SA-Cached,    Originator: Vlan2,    Connect-Source: Vlan2
MAX External SA Entry: 200000
MAX Peer External SA Entry: 20000
TTL Threshold: 0
SA Entry Hold Time: 350
Filters:
Redistribute_filter: Not set
SA-filter:
[IN]:    RP-list: None,    SG-list: None
[OUT]: Not Configured
SA-Request-Filter: Not Configured
Default Peer:
Not Configured
Mesh Group:
PLANET-1
```

The introduction of showed items:

Field Explaination
SA-Cached MSDP SA-Cached state.
Originator The RP interface of MSDP originated.
MAX External SA Entry

The max entries configured in MSDP configuration mode.
MAX Peer External SA Entry The max entries of each Peer.
TTL Threshold TTL Threshold.
SA Entry Hold Time The multicast source hold time of MSDP cache.
Redistribute_filter To establish the filter policy of SA message.
SA-filter [IN | OUT] The filter policy of receiving or sending SA message.
Default Peer Static RPF Peer.
Mesh Group The name and members of mesh group.

38.4.30 show msdp local-sa-cache

Command: show msdp local-sa-cache

Function: Display the information for local-sa-cache.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: Display the information for local-sa-cache.

Example:

```
Switch#show msdp local-sa-cache
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Source Address          Group Address          RP Address          TTL
5.5.5.9                 225.0.0.1              11.1.1.1            64
5.5.5.9                 225.0.0.2              11.1.1.1            64
5.5.5.9                 225.0.0.3              11.1.1.1            64
5.5.5.9                 225.0.0.4              11.1.1.1            64
```

38.4.31 show msdp peer

Command: show msdp peer {A.B.C.D}

Function: Show the configuration information in MSDP Mode.

Parameter: A.B.C.D: MSDP Peer Address.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information in MSDP configuration mode.

Example:

```
Switch#show msdp peer 31.1.1.3
MSDP Peer 31.1.1.3, AS 0,    Description:
Connection status:
      State: Established, Resets: 0,
      Connection Source: Not set, Connect address: 31.1.1.1
      Uptime (Downtime): 00h:07m:53s, SA messages received: 16
      TLV messages sent/received:         8/24
      SA messages incoming Rrjected:      0
      SA messages outgoing Rrjected:      0
    SA Filtering:
      Input filter Not Configured
      Output filter Not Configured
    SA-Requests:
      Input filter Not Configured
      Sending SA-Requests to peer: Disabled
Peer ttl threshold:    0
```

The introduction of showed items:

Field Explaination
MSDP Peer IP address of MSDP Peer.
AS Autonomous system number belonged toMSDP Peer.
State MSDP Peer state.
Connection source The interface used in local TCP connection.
Uptime(Downtime)

The uptime or downtime of MSDP peer.
Messages sent/received The statistics of messages sent and received from the Peer.
SA Filtering The filtering policy configured with Peers.
SA-Requests The configured filtering policy of SA requests.
SAs learned from this peer The SA numbers learned from MSDP Peers in the cache.
SAs limit The configured SA limit numbers with this MSDP Peer.

38.4.32 show msdp sa-cache

Command: show msdp sa-cache {<*source-address*> [<*group-address*>] | as-num <*sas-number*> | peer <*peer-address*>| rpaddr <*rp-address*>}

Function: Display the configuration information for cache-exterior source under MSDP.

Parameter: ***source-address:*** Source address;

group-address: Group address;

as-number: autonomous-system-number autonomous system number;

peer-address: Peer address;

rp-address: RP address.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the configuration information for cache-exterior source under MSDP.

Example:

```
Switch#show msdp sa-cache 30.30.30.1
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.
Cache SA Entry:
(S:30.30.30.1, G: 224.1.1.1, RP: 10.1.1.2),    AS: 0,    00h:00m:11s/00h:02m:19s
```

```
Learn From Peer:20.1.1.1,    RPF Peer: 10.1.1.10
SA Received: 10       Encapsulated data received: 0
grp flags: None       source flags:    EA, DE
```

The explanation of showed items:

field Explaination
(S, G, RP) running source message information(S, G, RP).
AS Num Autonomous system number.
update time SA message cache time.
expire time SA message expire time.
Learn From Peer The table is learned from the Peer.
RPF Peer RPF Peer of the entry.
SA Received SA message which include the entry.
Encapsulated data received The multicast message encapsulated in SA message.
grp flags The multicast group flag in the entry.
source flags The multicast source flag in the entry.

38.4.33 show msdp sa-cache summary

Command: show msdp sa-cache summary

Function: Show the summary of MSDP Cache.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the summary of MSDP Cache.

Example:

```
Switch#show msdp sa-cache summary

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Total number of SA Entries = 1
Total number of Sources = 1
Total number of Groups = 1
Total number of RPs = 1

Originator-RP        SA total       RPF peer
10.1.1.2                    1          10.1.1.10

AS-num      SA total
0             1
```

The introduction of showed items:

Field Explaination
Total number of SA Entries Total number of SA entries in the cache.
Total number of Sources Total number of different multicast sources in the cache.
Total number of Groups Total number of different multicast groups in the cache.
Total number of RPs Total number of different RP in the cache.
Originator-RP Originated RP address.

SA total Total number of received SA message from RP.
RPF peer The RPF Peer address of corresponding RP.
AS-num Autonomous system number.

38.4.34 show msdp statistics

Command: show msdp statistics peer [*Peer-address*]

Function: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.

Parameter: Peer-address: Show the statistics of messages from specified Peer.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.

Example:t

```
Switch#show msdp sta peer 2.2.2.4

MSDP Peer Statistics :
Peer   2.2.2.4 ,    AS is   0 ,    State is   Inactive
     TLV Rcvd :      76 total
                     39 keepalives,         37 SAs
                      0 SA Requests,        0 SA responses
     TLV Send :      80 total
                     41 keepalives,         39 SAs
                      0 SA Requests,        0 SA responses
     SA   msgs :     37 received,      39 sent
```

The introduction of showed items:

Field Explaination
Peer MSDP Peer address.
AS Autonomous system number.
State MSDP Peer state.

TLV Rcvd The TLV type and statistics of Peer received.
TLV Send The TLV type and statistics of Peer sent
SA msgs The SA message statistics of Peer received and send.

38.4.35 show msdp summary

Command: show msdp summary

Function: Show the summary of MSDP.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the summary of MSDP.

Example:

```
Switch#show msdp summary

Maximum External SA's Global : 20000
MSDP Peer Status Summary
Peer Address AS State     Uptime/     Reset  Peer  Active  Cfg.Max      TLV
                          Downtime    Count  Name  SA      Cnt Ext.SAs  recv/sent
 2.2.2.4     0  Established THU JAN 01 00:00:00  10      0            121/100
```

The introduction of showed items:

Field Explaination
Peer Address IP address of MSDP Peer.
AS Autonomous system number belonged toMSDP Peer.
State MSDP Peer state.
Uptime/Downtime The uptime or downtime of MSDP peer.

Reset Count The reset count of MSDP Peer.
Peer Name The description of MSDP Peer.
Active SA The numbers of active SA.
TLV sent/received The statistics of TLV messages sent and received from the Peer.

38.4.36 shutdown

Command: shutdown

no shutdown

Function: Disable specified MSDP Peer.

Parameter: None.

Command Mode: MSDP Peer Configuration Mode.

Default: Enabled.

Usage Guide: When configuring a MSDP Peer with multiple commands, sometimes it is required that these commands should be effect together but not one by one. The shutdown command can be used to disable the peer before configuration and the no shutdown used after configuration in order to make the peer configuration effect together. The shutdown command will remove all the TCP sessions with the specified MSDP Peer as well as the statistics.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# shutdown
```

38.4.37 ttl-threshold

Command: ttl-threshold <*ttl*>

no ttl-threshold

Function: To configure the minimum TTL value of multicast source encapsulated in SA message.

Parameter: *ttl*：minimum TTL value，range between 1 to 255.

Command Mode: MSDP Configuration Mode.

Default: TTL value will not be filtered when TTL value is 0.

Usage Guide: The redistribution of multicast datagrams can be controlled through the TTL value. SA messages will be advertised only if the TTL value in the packet is less than the TTL threshold.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#ttl-threshold 10
```

38.5 Commands for ANYCAST RP v4

38.5.1 debug pim anycast-rp

Command: debug pim anycast-rp

no debug pim anycast-rp

Function: Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.

Command Mode: Admin Mode.

Default: The debug switch of ANYCAST RP is disabled by default.

Usage Guide: This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example:

```
Switch#debug pim anycast-rp
```

38.5.2 ip pim anycast-rp

Command: ip pim anycast-rp

no ip pim anycast-rp

Function: Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.

Command Mode: Global Configuration Mode.

Default: The switch will not enable the ANYCAST RP by default.

Usage Guide: This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.

Example: Enable ANYCAST RP in global configuration mode.

```
Switch(config)#ip pim anycast-rp
```

38.5.3 ip pim anycast-rp

Command: ip pim anycast-rp *<anycast-rp-addr> <other-rp-addr>*

no ip pim anycast-rp *<anycast-rp-addr> <other-rp-addr>*

Function: Configure ANYCAST RP address（ARA）and the unicast addresses of other RP communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.

Parameters: *anycast-rp-addr*: RP address, the absence of the candidate interface in accordance with the address is allowed.

***other-rp-addr*:** The unicast address of other RP communicating with this router(as a RP).

Command Mode: Global Configuration Mode.

Default: There is no configuration by default.

Usage Guide:

1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.

2. Configure the other-rp-address of other RP communicating with this router(as a RP). The unicast address identifies other RP, and is used to communicate with the local router.

3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source(S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.

4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received, it should be forwarded to all of these other RP one by one.

Example: Configure other-rp-address in global configuration mode.

```
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2
```

38.5.4 ip pim anycast-rp self-rp-address

Command: ip pim anycast-rp self-rp-address <*self-rp-addr*>

no ip pim anycast-rp self-rp-address

Function: Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.

Parameters: *self-rp-addr*：The unicast address used by this router (as a RP) to communicate with other RP.

Command Mode: Global Configuration Mode.

Default: No self-rp-address is configured by default.

Usage Guide:

1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.

2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.

3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.

Example: Configure the self-rp-address of this router in global configuration mode.

```
Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1
```

38.5.5 ip pim rp-candidate

Command: ip pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A.B.C.D*>] [<*priority*>]

no ip pim rp-candidate

Function: Add a Loopback interface as a RP candidate interface based on the original PIM-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.

Parameters: *index*: Loopback interface index, whose range is <1-1024>.

***vlan-id*:** the Vlan ID.

***ifname*:** the specified name of the interface.

A.B.C.D/M: the ip prefix and mask.

***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.

Command Mode: Global Configuration Mode.

Default Setting: No RP interface is configured by default.

Usage Guide: In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ip pim rp-candidate” command can be used to cancel the RP candidate.

Example: Configure Loopback1 interface as the RP candidate interface in global configuration mode.

```
Switch(config)#ip pim rp-candidate loopback1
```

38.5.6 show debugging pim

Command: show debugging pim

Command Mode: Admin Mode.

Usage Guide: The current state of ANYCAST RP debug switch.

Example:

```
witch(config)#show debugging pim

Debugging status:
  PIM anycast-rp debugging is on
```

38.5.7 show ip pim anycast-rp first-hop

Command: show ip pim anycast-rp first-hop

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.

Example:

```
Switch(config)#show ip pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (192.168.1.136, 224.1.1.1)
 Local        .l.....................
```

Display Explanation
Entries The number of all kinds of entries.
INCLUDE The information of mrt generated in the first hop RP.

38.5.8 show ip pim anycast-rp non-first-hop

Command: show ip pim anycast-rp non-first-hop

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.

Example:

```
Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (192.168.10.120, 225.1.1.1)
 Local        .l.....................
```

Display Explanation
Entries The number of all kinds of entries.
INCLUDE The mrt information created in the first hop RP.

38.5.9 show ip pim anycast-rp status

Command: show ip pim anycast-rp status

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured ANYCAST RP set.

Example:

```
Switch(config)#show ip pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:192.168.3.2

anycast-rp address: 1.1.1.1
      other rp unicast rp address: 192.168.2.1
      other rp unicast rp address: 192.168.5.1

anycast-rp address: 192.168.1.4
      other rp unicast rp address: 192.168.2.1

--------------------------------
```

Display Explanation
anycast-rp: Whether the ANYCAST RP switch is globally enabled.
self-rp-address: The configured self-rp-address.

anycast-rp address: The configured anycast-rp-address.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.
anycast-rp address: The configured anycast-rp-address*.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.

38.6 Commands for PIM-SSM

38.6.1 ip multicast ssm

Command: ip multicast ssm {default|range <*access-list-number* >}

no ip multicast ssm

Function: Configure the range of pim ssm multicast address. The "**no ip multicast ssm**" command deletes configured pim ssm multicast group.

Parameter: default: indicates the default range of pim ssm multicast group is 232/8.

<access-list-number > is the applying access-list number, it ranges from 1 to 99.

Default: Do not configure the range of pim ssm group address.

Command Mode: Global Mode.

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ip pim multicasting succeed. This command can't work with DVMRP.

3. Access-list can't used the lists created by ip access-list, but the lists created by access-list.

4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ip pim ssm can release the bondage.

5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with IGMP (must) and multicast source DR or RP (at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

```
Switch (config)#ip multicast ssm range 23
```

38.7 Commands for DVMRP

38.7.1 debug dvmrp

Command: debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]|nsm|mfc|mib|timer[probe[probe-timer|neighbor-expiry-timer]|prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

Function: Display DVMRP protocol debugging message; the "**no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm| mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]| route[report-timer|flash-upd-timer|route-expiry-timer| route-holdown-timer|route-burst-timer]] |packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]**" command disenables this debugging switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable this switch, and display DVMRP protocol executed relevant messages.

38.7.2 ip dvmrp enable

Command: ip dvmrp enable

no ip dvmrp

Function: Configure to enable DVMRP protocol on interface; the "**no ip dvmrp**" command disenables DVMRP protocol.

Parameter: None

Default: Disable DVMRP Protocol

Command Mode: Interface Configuration Mode

Usage Guide: The interface processes DVMRP protocol messages, only executing DVMRP protocol on interface.

Example: Enable DVMRP Protocol on interface vlan1.

Switch (config)#interface vlan 1
Switch(Config-If-vlan1)#ip dvmrp enable

38.7.3 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>

no ip dvmrp metric

Function: Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.

Parameter: <*metric_val*> is metric value, value range from 1 to 31

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: The routing information in DVMRP report messages includes a groupsource network and metric list. After configuring interface DVMRP report message metric value, it makes all received routing entriy from the interface adding configured interface metric value as new metric value of the routing. The metric value applies to calculate posion reverse, namely ensuring up-downstream relations. If the metric value of some route on the switch is not less than 32, it explains the route can be reach. If it is downstream of some route after calculation and judgment, it will transmit report message included the route to upstream. The route metric increases 32 based on original value in order to indicate downstream itself.

Example: Configure interface DVMRP report message metric value: 2

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dvmrp metric 2
```

38.7.4 ip dvmrp multicast-routing

Command: ip dvmrp multicast-routing

no ip dvmrp multicast-routing

Function: Globally enable DVMRP protocol; the "no ip dvmrp multicast-routing" command globally disenables DVMRP protocol

Parameter: None

Default: Default

Command Mode: Global Mode

Usage Guide: Dvmrp multicast-protocol can enable after globally execute the command

Example:

```
Switch (config)#ip dvmrp multicast-routing
```

38.7.5 ip dvmrp output-report-delay

Command: ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>]

no ip dvmrp output-report-delay

Function: Configure the delay of DVMRP report message transmitted on interface and transmitted message quantity every time, the "**no ip dvmrp output-report-delay**" command restores default value.

Parameter: <*delay_val*> is the delay of periodically transmitted DVMRP report message, value range from 1s to 5s.

<burst_size> is a quantity of transmitted message every time, value range from 1 to 65535

Default: Default the delay of transmitted DVMRP report message as 1s, default: transmitting two messages every time.

Command Mode: Interface Configuration Mode

Usage Guide: Avoid message burst if setting an appropriate delay.

Example:

```
Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024
```

38.7.6 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Function: Configure to reject neighbor ship with DVMRP router of non pruning/grafting on the interface, the "**no ip dvmrp reject-non-pruners**" command restores neighbor ship can be established.

Parameter: None

Default: Default

Command Mode: Interface Configuration Mode

Usage Guide: The command determines if it will establish neighboringship with DVMRP router of non pruning/grafting or not.

Example:

```
Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners
```

38.7.7 ip dvmrp tunnel

Command: ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*>

no ip dvmrp tunnel {**<*index*> |<*src-ip*> <*dst-ip*>}**

Function: Configure a DVMRP tunnel; the "**no ip dvmrp tunnel** {**<*index*> |<*src-ip*> <*dst-ip*>}**" command deletes a DVMRP tunnel.

Parameter: <*src-ip*> is source IP address,

<dst-ip> is remote neighbor IP address,

<index> is tunnel index number, value range from 1 to 65535.

Default: Do not Configure DVMRP tunnel.

Command Mode: Global Mode

Usage Guide: Because not all of switches support multicast, DVMRP supports tunnel multicast communication. The tunnel is a way of transmitted multicast data packet among DVMRP switches partitioned off switches without supporting multicast routing. It acts as a virtual network between two DVMRP switches. Multicast data packets packed in unicast data packets, directly are transmitted to next supporting multicast switch. DVMRP protocol equally deal with tunnel interface and general physical interface. After configuring no ip dv multicast-routing, all of the tunnel configurations are deleted.

Example:

```
Switch(config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1
```

38.7.8 show ip dvmrp

Command: show ip dvmrp

Function: Display DVMRP protocol information.

Parameter: None

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display some total statistic information of DVMRP protocol

Example:

```
Switch#show ip dvmrp
DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001
DVMRP Daemon Uptime: 17:37:03
DVMRP Number of Route Entries: 2
DVMRP Number of Reachable Route Entries: 2
DVMRP Number of Prune Entries: 1
DVMRP Route Report Timer: Running
DVMRP Route Report Timer Last Update: 00:00:56
DVMRP Route Report Timer Next Update: 00:00:04
DVMRP Flash Route Update Timer: Not Running
```

38.7.9 show ip dvmrp interface

Command: show ip dvmrp interface [<*ifname*>]

Function: Display DVMRP interface

Parameter: <*ifname*> is interface name, namely displaying configured interface information of specified interface.

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Example:

```
Switch #show ip dvmrp in vlan4
Address          Interface   Vif    Ver.   Nbr   Type    Remote
                             Index         Cnt           Address
13.1.1.3         Vlan1       1      v3.ff  0     BCAST   N/A
10.1.35.3        Vlan2       0      v3.ff  0     BCAST   N/A
```

```
Switch #
```

Displayed Information	Explanations

Address Address
Interface Interface corresponding physical interface name
Vif Index Virtual interface index
Ver Interface supporting version
Nbr Cnt Neighbor count
Type Interface type
Remote Address Remote address

38.7.10 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [{*<ifname>* *<A.B.C.D>* [detail]}|{ *<ifname>*[detail]}|detail]

Function: Display DVMRP neighbor.

Parameter: ***<ifname>*** is interface name, namely displaying neighbor information of specified interface.

Default: Do not display (Off).

Command Mode: Any Configuration Mode

Example: Display interface vlan1 neighbor on Ethernet.

```
Switch #show ip dvmrp neighbor
Neighbor          Interface   Uptime/Expires          Maj  Min  Cap
Address                                               Ver  Ver  Flg
10.1.35.5         Vlan2       00:00:16/00:00:29       3    255  2e
```

Displayed Information Explanations
Neighbor Address Neighbor address
Interface

Detect the neighbor's interface
Uptime/Expires The neighbor uptime/expire time
Maj Ver Major version
Min Ver Mini version
Cap Flg Capacity flag

38.7.11 show ip dvmrp prune

Command: show ip dvmrp prune [{group <A.B.C.D> [detail]}|{source <A.B.C.D/M> group <A.B.C.D> [detail]}|{source <A.B.C.D/M> [detail] }|detail]

Function: Display DVMRP message forwarding item.

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: This command applies to display DVMRP multicast forwarding item, namely multicast forwarding table calculated by dvmrp protocol.

Example:

```
Switch#show ip dvmrp prune
Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init
Source          Mask Group          State  FCR Exptime   Prune/Graft
Address         Len  Address                Cnt           ReXmit-Time
13.1.1.0        24   239.0.0.1      ..... 1  01:59:56      Off
```

Displayed Information Explanations
Source Address Source address
Mask Len Mask length
Group Address

Group address
State Table item state
FCR Exptime FCR expire time
Prune/Graft ReXmit-Time Prune expire time/ Graft retransmit time

38.7.12 show ip dvmrp route

Command: show ip dvmrp route [{<A.B.C.D/M>[detail]}|{nexthop <A.B.C.D>[detail]}|{best-match <A.B.C.D> [detail]}|detail]

Function: Prune expire time/ Graft retransmit time

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display DVMRP routing table item; DVMRP maintains individual unicast routing table to check RPF.

Example: Display DVMRP routiing.

```
Switch #show ip dvmrp route
Flags: N = New, D = DirectlyConnected, H = Holddown
Network          Flags Nexthop    Nexthop              Metric  Uptime    Exptime
                       Xface      Neighbor
10.1.35.0/24     .D.   Vlan2      Directly Connected   1       00:11:16  00:00:00
13.1.1.0/24      .D.   Vlan1      Directly Connected   1       00:10:22 00:00:00
```

Displayed Information Explanations
Network Target net segment or address and mask
Flags Routing state flag
Nexthop Xface Next hop interface address

Nexthop Neighbor Next hop neighbor
Metric Routing metric value
Uptime Routing uptime
Exptime Routing expire time

38.8 Commands for DCSCM

38.8.1 access-list (Multicast Destination Control)

Command: access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure destination control multicast access-list, the "**no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: <6000-7999>: destination control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address.

<source-wildcard>: multicast source address wildcard character..

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example:

Switch(config)#

```
Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
Switch(config)#
```

38.8.2 access-list (Multicast Source Control)

Command: access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure source control multicast access-list; the "**no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: <5000-5099>: source control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address..

<source-wildcard>: multicast source address wildcard character.

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast source control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example:

```
Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
```

38.8.3 ip multicast destination-control access-group

Command: ip multicast destination-control access-group <6000-7999>

no ip multicast destination-control access-group <6000-7999>

Function: Configure multicast destination-control access-list used on interface, the "**no ip multicast destination-control access-group <6000-7999>**" command deletes the configuration.

Parameter: <6000-7999>: destination-control access-list number.

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example:

```
Switch(config)#inter e 1/4
Switch(Config-If-Ethernet 1/4)#ip multicast destination-control access-group 6000
Switch (Config-If-Ethernet1/4)#
```

38.8.4 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified net segment, the "**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**" command deletes this configuration.

Parameter: <IPADDRESS/M>: IP address and mask length;

<6000-7999>: Destination control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.

Example:

```
Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000
```

38.8.5 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control <1-4094> <macaddr>access-group <6000-7999>

no ip multicast destination-control <1-4094> <macaddr>access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified vlan-mac, the "**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**"command deletes this configuration.

Parameter: <1-4094>: VLAN-ID;

<macaddr>: Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";

<6000-7999>: Destination-control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example:

```
Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000
```

38.8.6 ip multicast policy

Command: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>

no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configure multicast policy, the "**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**" command deletes it.

Parameter: <IPADDRESS/M>: are multicast source address, mask length, destination address, and mask length separately.

<priority>: specified priority, range from 0 to 7

Default: None

Command Mode: Global Mode

Usage Guide: The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously. Carefully, the packet transmitted in UNTAG mode does not modify its priority.

Example:

```
Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7
```

38.8.7 ip multicast source-control

Command: ip multicast source-control

no ip multicast source-control

Function: Configure to globally enable multicast source control, the "**no ip multicast source-control**" command restores global multicast source control disabled.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded.

Example:

```
Switch(config)#ip multicast source-control
```

38.8.8 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>

no ip multicast source-control access-group <5000-5099>

Function: Configure multicast source control access-list used on interface, the “no ip multicast source-control access-group <5000-5099>“ command deletes the configuration.

Parameter: <5000-5099>: Source control access-list number**.**

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.

Example:

```
Switch (config)#interface ethernet1/4
Switch (Config-If-Ethernet1/4)#ip multicast source-control access-group 5000
Switch (Config-If-Ethernet1/4)#
```

38.8.9 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPV4 and IPV6 multicast destination control. After configuring this command, multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPV4 and IPV6 multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only after globally enabling the multicast destination control, the other destination control configuration can take effect. The destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING, MLD-SNOOPING and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.

Example:

```
Switch(config)# multicast destination-control
Switch(config)#
```

38.8.10 show ip multicast destination-control

Command: show ip multicast destination-control [detail]

show ip multicast destination-control interface <Interfacename> [detail]

show ip multicast destination-control host-address <ipaddress> [detail]

show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function: Display multicast destination control

Parameter: detail: expresses if it display information in detail or not..

<interfacename>: interface name or interface aggregation name, such as Ethernet1/1, port-channel 1 or ethernet1/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast destination control rules of configuration, including detail option, and access-list information applied in detail.

Example:

```
Switch (config)#show ip multicast destination-control
ip multicast destination-control is enabled
ip multicast destination-control 11.0.0.0/8 access-group 6003
ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001
multicast destination-control access-group 6000 used on interface Ethernet1/13
```

```
switch(config)#
```

38.8.11 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list

show ip multicast destination-control access-list <6000-7999>

Function: Display destination control multicast access-list of configuration.

Parameter: <6000-7999>: access-list number.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays destination control multicast access-list of configuration.

Example:

```
Switch# sh ip multicast destination-control acc
access-list 6000 deny ip any any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255
```

38.8.12 show ip multicast policy

Command: **show ip multicast policy**

Function: Display multicast policy of configuration

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast policy of configuration

Example:

```
Switch#show ip multicast policy
ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5
```

38.8.13 show ip multicast source-control

Command: **show ip multicast source-control [detail]**

show ip multicast source-control interface <Interfacename> [detail]

Function: Display multicast source control configuration

Parameter: detail: expresses if it displays information in detail.

<Interfacename>: interface name, such as Ethernet 1/1 or ethernet1/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.

Example:

```
Switch#show ip multicast source-control detail
ip multicast source-control is enabled
Interface Ethernet1/13 use multicast source control access-list 5000
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

38.8.14 show ip multicast source-control access-list

Command: **show ip multicast source-control access-list**

show ip multicast source-control access-list <5000-5099>

Function: Display source control multicast access-list of configuration

Parameter: <5000-5099>: access-list number

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays source control multicast access-list of configuration

Example:

```
Switch#sh ip multicast source-control access-list
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

38.9 Commands for IGMP

38.9.1 clear ip igmp group

Command: clear ip igmp group [A.B.C.D | IFNAME]

Function: Delete the group record of the specific group or interface.

Parameters: A.B.C.D the specific group address; IFNAME the specific interface.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ip igmp group
```

Relative Command: show ip igmp group

38.9.2 debug igmp event

Command: debug igmp event

no debug igmp event

Function: Enable debugging switch of IGMP event; the "**no debug igmp event**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable debugging switch if querying IGMP event information

Example:

```
Switch# debug igmp event
igmp event debug is on
```

```
Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out
```

38.9.3 debug igmp packet

Command: debug igmp packet

no debug igmp packet

Function: Enable debugging switch of IGMP message information; the "**no debug igmp packet**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the debugging switch if querying IGMP message information.

Example:

```
Switch# debug igmp packet
igmp packet debug is on
Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0
```

```
02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0
.0.0
02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0
02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0
.0.0
```

38.9.4 ip igmp access-group

Command: ip igmp access-group {<*acl_num* | *acl_name*>}

no ip igmp access-group

Function: Configure interface to filter IGMP group; the "**no ip igmp access-group**" command cancels the filter condition

Parameter: {<acl_num | acl_name>} is SN or name of access-list, value range of **acl_num** is from 1 to 99.

Default: Default no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure interface to filter groups, permit or deny some group joining.

Example: Configure interface vlan1 to permit group 224.1.1.1, deny group 224.1.1.2.

```
Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0
Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp access-group 1
```

38.9.5 ip igmp immediate-leave

Command: ip igmp immediate-leave group-list {<number>|<name>}

no ip igmp immediate-leave

Function: Configure IGMP working in immediate-leave mode, that is, when the host transmits member identity report of equivalent to leave a group, router does not transmit query, it directly confirms there is no member of this group in subnet; the "**no ip igmp immediate-leave**" command cancels immediate-leave mode.

Parameter: *<number>* is access-list SN, value is from 1 to 99.

<name> is access-list name.

Default: Interface default and no immediate-leave group of configuration after finished product

Command Mode: Interface Configuration Mode

Usage Guide: The command only can apply in only one host condition in subnet.

Example: Configure immediate-leave mode on access-group list 1

```
Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1
```

Switch (Config-if-Vlan1)#

38.9.6 ip igmp join-group

Command: ip igmp join-group <*A.B.C.D* >

no ip igmp join-group <*A.B.C.D* >

Function: Configure interface to join some IGMP group; the “no ip igmp join-group” command cancels this join

Parameter: <*A.B.C.D*>: is group address

Default: Do not join

Command Mode: Interface Configuration Mode

Usage Guide: When the switch is the HOST, the command configures HOST to join some group; that is, if configuring the interface join-group 224.1.1.1, it will transmit IGMP member report including group 224.1.1.1 when the switch receives IGMP group query transmitted by other switches. Carefully, it is the diffence between the command and **ip igmp static-group** command.

Example: Configure join-group 224.1.1.1 on interface vlan1.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp join-group 224.1.1.1

38.9.7 ip igmp last-member-query-interval

Command: ip igmp last-member-query-interval <interval>

no ip igmp last-member-query-interval

Function: Configure interval of specified group query transmitting on interface; the “**no ip igmp last-member-query-interval**” command cancels the value of user manual configuration, and restores default value.

Parameter:<*interval*> is interval of specified group query, range from 1000ms to 25500ms; the value is integer times of 1000ms, namely if input value is not integer times of 1000ms, the system automatically changes to integer times of 1000ms.

Default: 1000ms

Command Mode: Interface Configuration Mode

Example: Configure interface vlan1 IGMP last-member-query-interval to 2000.

Switch (config)#int vlan 1
Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000

38.9.8 ip igmp limit

Command: ip igmp limit <state-count>

no ip igmp limit

Function: Configure limit IGMP state-count on interface; the "**no ip igmp limit**" command cancels the value of user manual configuration, and restores default value.

Parameter: ***<state-count>*** is maximum IGMP state reserved by interface, range from 1 to 65000

Default: 0, no limit.

Command Mode: Interface Configuration Mode

Usage Guide: After configuring maximum state state-count, interface only saves states which are not more than state-count groups and sources. If it reaches upper limit of state-count, it does not deal with when receiving related new group member identity report. If it has saved some IGMP group states before configuring the command, it deletes all of the states, and then immediately transmits IGMP general query to collect the member identity report which is not more than state-count group. Static state and static source are not in the limit

Example: Configure interface vlan1 IGMP limit to 4000.

```
Switch (config)#int vlan 1
Switch (Config-if-vlan1)#ip igmp limit 4000
```

38.9.9 ip igmp query-interval

Command: ip igmp query-interval <*time_val*>

no ip igmp query-interval

Function: Configure interval of periodically transmitted IGMP query information; the "**no ip igmp query-interval**" command restores default value.

Parameter: ***<time_val>*** is interval of periodically transmitted IGMP query information, value range from 1s to 65535s.

Default: Default interval of periodically transmitted IGMP query information to 125s.

Command Mode: Interface Configuration Mode

Usage Guide: Periodically transmitting IGMP query information on interface when some interface enables some group multicast protocol. The command applies to configure this query period time.

Example: Configure interval of periodically transmitted IGMP query message to 10s

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query-interval 10
```

38.9.10 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <*time_val*>

no ip igmp query- max-response-time

Function: Configure IGMP query-max-response-time of interface; the "**no ip igmp query-max-response-time**" command restores default value.

Parameter: <***time_val***> is IGMP query-max-response-time of interface, value range from 1s to 25s

Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: After the switch receives a query message, the host will configure a timer for its affiliated

every multicast group, the value of timer is selected random from 0 to maximum response time, the host will transmit member report message of the multicast group. Reasonable configuring maximum response time, it can make host quickly response query message. The router can also quickly grasp the status of multicast group member.

Example: configure the maximum period responding to the IGMP query messages to 20s

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query- max-response-time 20
```

38.9.11 ip igmp query-timeout

Command: ip igmp query-timeout <*time_val*>

no ip igmp query-timeout

Function: Configure IGMP query timeout of interface; the "**no ip igmp query-timeout**" command restores default value.

Parameter: <***time_val***> is IGMP query-timeout, value range from 60s to 300s.

Default: 255s.

Command Mode: Interface Configuration Mode

Usage Guide: When multi-running IGMP switches are exist on sharing network, a switch will be voted as query processor on the sharing network, and other switches will be a timer monitoring the state of query processor; It still does not receive query message transmitting by query processor over query time-out, thus it re-votes another switch as new query processor.

Example: Configure timeout of IGMP query message on interface to 100s.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query-timeout 100
```

38.9.12 ip igmp robust-variable

Command: ip igmp robust-variable <value>

no ip igmp robust-variable

Function: Configure the robust variable value，the "**no ip igmp robust-variable**" command restores default value.

Parameter: value：range from 2 to 7.

Command Mode: Interface Configuration Mode

Default: 2.

Usage Guide: It is recommend to use the default value.

Example:

```
Switch (config-if-vlan1)#ip igmp robust-variable 3
```

38.9.13 ip igmp static-group

Command: ip igmp static-group <*A.B.C.D* > [source <*A.B.C.D* >]

no ip igmp static -group <*A.B.C.D* > [source <*A.B.C.D* >]

Function: Configure interface to join some IGMP static group; the “no ip igmp static-group” command cancels this join.

Parameter: <*A.B.C.D*> is group address;

Source **<*A.B.C.D*>** expresses SSM source address of configuration.

Default: Do not join static group

Command Mode: Interface Configuration Mode

Usage Guide: When configuring some interface to join some static group, it will receives about the multicast packet of the static group whether the interface has a real receiver or not; that is, if configuring the interface to join static group 224.1.1.1, the interface always receives about multicast packet about group 224.1.1.1 whether the interface has a receiver or not. Carefully, it is the difference between the command and ip igmp join-group command.

Example: Configure static-group 224.1.1.1 on interface vlan1.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp static-group 224.1.1.1

38.9.14 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configure IGMP version on interface; the “**no ip igmp version**” command restores default value.

Parameter: <***version***> is IGMP version of configuration, currently supporting version 1, 2 and 3.

Default: version 2.

Command Mode: Interface Configuration Mode

Usage Guide: The command mainly applies to supply upward compatibility of the different version; it is not communicated between version 1 and version 2, therefore it must configure to the same version IGMP in the same network. When other routers which are not upgraded to IGMPv3 on interface-connected subnet need to join member identity collection of subnet IGMP together, the interface is configured to corresponding version.

Example: Configure IGMP on interface to version 3.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp version 3

38.9.15 show ip igmp groups

Command: show ip igmp groups [<*A.B.C.D*>] [*detail*]

Function: Display IGMP group information

Parameter: <*group_addr*> is group address, namely querying specified group information; Detail expresses group information in detail

Default: Do not display

Command Mode: Admin Mode

Example:

```
Switch (config)#show ip igmp groups
IGMP Connected Group Membership (2 group(s) joined)
Group Address      Interface          Uptime      Expires     Last Reporter
226.0.0.1          Vlan1              00:00:01    00:04:19    1.1.1.1
239.255.255.250    Vlan1              00:00:10    00:04:10    10.1.1.1
```

```
Switch#
```

Displayed Information Explanations
Group Address Multicast group IP address
Interface Interface affiliated with multicast group
Uptime Multicast group uptime
Expires Multicast group expire time
Last Reporter Last reporter to the host of the multicast group

```
Switch (config)#show ip igmp groups 234.1.1.1 detail
IGMP Connect Group Membership (2 group(s) joined)
Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host Pres
ent, V2 - V2 Host Present
Interface:          Vlan1
Group:              234.1.1.1
Flags:
Uptime:             00:00:19
Group Mode:    INCLUDE
Last Reporter:  10.1.1.1
Exptime:        stopped
Source list: (2 members    S - Static)
Source Address     Uptime      v3 Exp      Fwd    Flags
```

```
1.1.1.1          00:00:19  00:04:01  Yes
2.2.2.2          00:00:19  00:04:01  Yes
```

Displayed Information Explanations
Group Mutlicast group IP address
Interface Interface affiliated with Mutlicast group
Flags Group property flag
Uptime Mutlicast group uptime
Group Mode Group mode, including INCLUDE and EXCLUDE. Group V3 will be available, group V1 and group V2 are regards as EXCLUDE mode.
Exptime Mutlicast group expire time
Last Reporter Last reporter to the host of the Mutlicast group
Source Address Source address of this group
V3 Exp Source expire time
Fwd If the data of the source is forwarded or not.
Flags Source property flag

38.9.16 show ip igmp interface

Command: show ip igmp interface {vlan <*vlan_id*>|<*ifname*>}

Function: Display related IGMP information on interface.

Parameter: <*ifname*> is interface name, namely displaying IGMP information of specified interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display interface vlan1 IGMP message on Ethernet.

```
Switch (config)#show ip igmp interface Vlan1
Interface Vlan1(2005)
 Index 2005
 Internet address is 10.1.1.2
 IGMP querier
 IGMP current version is V3, 2 group(s) joined
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 ms
 Group Membership interval is 260 seconds
 IGMP is enabled on interface
```

38.10 Commands for IGMP Snooping

38.10.1 clear ip igmp snooping vlan

Command: clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]

Function: Delete the group record of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; A.B.C.D the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ip igmp snooping vlan 1 groups
```

Relative Command: show ip igmp snooping vlan <1-4094>

38.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port

Command: clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]

Function: Delete the mrouter port of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted mrouter port of the specific VLAN.

Example: Delete mrouter port in vlan 1.

```
Switch# clear ip igmp snooping vlan 1 mrouter-port
```

Relative Command: show ip igmp snooping mrouter-port

38.10.3 debug igmp snooping all/packet/event/timer/mfc

Command: debug igmp snooping all/packet/event/timer/mfc

no debug igmp snooping all/packet/event/timer/mfc

Function: Enable the IGMP Snooping switch of the switch; the "**no debug igmp snooping all/packet/event/timer/mfc**" disables the debugging switch.

Command Mode: Admin Mode

Default: IGMP Snooping debugging switch is disabled on the switch by default.

Usage Guide: The command is used for enable the IGMP Snooping debugging switch of the switch, switch IGMP data packet message can be shown with "packet" parameter, event message with "event", timer message with "time", downsending hardware entries message with "mfc", and all debugging messages with "all".

38.10.4 ip igmp snooping

Command: ip igmp snooping

no ip igmp snooping

Function: Enable the IGMP Snooping function; the "**no ip igmp snooping**" command disables this function.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping, that is permission every vlan config the function of IGMP snooping. The "**no ip igmp snooping**" command disables this function.

Example: Enable IGMP Snooping.

```
Switch(config)#ip igmp snooping
```

38.10.5 ip igmp snooping vlan

Command: ip igmp snooping vlan *<vlan-id>*

no ip igmp snooping vlan *<vlan-id>*

Function: Enable the IGMP Snooping function for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameter: *<vlan-id>* is the VLAN number.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: To configure IGMP Snooping on specified vlan, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified vlan with the "**no ip igmp snooping vlan <vlan-id>**" command.

Example: Enable IGMP Snooping for VLAN 100 in Global Mode.

```
Switch(config)#ip igmp snooping vlan 100
```

38.10.6 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan <*vlan-id*> immediate-leave

no ip igmp snooping vlan <*vlan-id*> immediate-leave

Function: Enable the IGMP fast leave function for the specified VLAN; the "**no ip igmp snooping vlan <*vlan-id*> immediate-leave**" command disables the IGMP fast leave function.

Parameter: <*vlan-id*> is the VLAN number specified.

Command mode: Global Mode

Default: This function is disabled by default.

Usage Guide: Enable immediate-leave function of the IGMP Snooping in specified vlan; the"no" form of this command disables the immediate-leave function of the IGMP Snooping.

Example: Enable the IGMP fast leave function for VLAN 100.

```
Switch(config)#ip igmp snooping vlan 100 immediate-leave
```

38.10.7 ip igmp snooping vlan l2-general-querier

Command: ip igmp snooping vlan < *vlan-id* > l2-general-querier

no ip igmp snooping vlan < *vlan-id* > l2-general-querier

Function: Set this vlan to layer 2 general querier.

Parameter: ***vlan-id***: is ID number of the VLAN, ranging between <1-4094>.

Command Mode: Global mode

Default: VLAN is not as the IGMP Snooping layer 2 general querier.

Usage Guide: It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this vlan before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.

Comment: There are three paths IGMP snooping learn mrouter

1 Port receives the IGMP query messages

2 Port receives multicast protocol packets, and supports DVMRP, PIM

3 Static configured port

38.10.8 ip igmp snooping vlan l2-general-querier-source

Command: ip igmp snooping vlan <vlanid> L2-general-query-source <A.B.C.D>

no ip igmp snooping vlan <vlanid> L2-general-query-source

Function: Configure source address of query of igmp snooping

Parameters: <vlanid>: the id of the vlan, with limitation to <1-4094>. **<A.B.C.D>** is the source address of the query operation.

Command Mode: Global mode.

Default; 0.0.0.0

Usage Guide: It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.

Example:

```
Switch(config)#ip igmp snooping vlan 2 L2-general-query-source 192.168.1.2
```

38.10.9 ip igmp snooping vlan l2-general-querier-version

Command: ip igmp snooping vlan <vlanid> L2-general-query-version <version>

Function: Configure igmp snooping.

Parameters: vlan-id is the id of the VLAN, limited to <1-4094>. **version** is the version number, limited to <1-3>.

Command Mode: Global mode.

Default: version 3.

Usage Guide: When the switch is connected to V1 and V2 capable environment, and for vlan which has source of layer 2 query configuration, the vlan can be queried only if the version number has been specified. This command is used to query the layer 2 version number.

Example:

```
Switch(config)#ip igmp snooping vlan 2 L2-general-query-version 2
```

38.10.10 ip igmp snooping vlan limit

Command: ip igmp snooping vlan <*vlan-id*> limit {group <*g_limit*> | source <*s_limit*>}

no ip igmp snooping vlan <*vlan-id*> limit

Function: Configure the max group count of vlan and the max source count of every group. The "**no ip igmp snooping vlan <*vlan-id*> limit**" command cancels this configuration.

Parameter: <*vlan-id*> is the VLAN number.

g_limit：<1-65535>, max number of groups joined.

s_limit：<1-65535>, max number of source entries in each group, consisting of include source and exclude source.

Command mode: Global Mode.

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, IGMP snooping must be enabled on vlan. The "no" form of this command restores the default other than set to "no limit". For the safety considerations, this command will not be configured to "no limit". It is recommended to use default value and if layer 3 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.

Example:

```
Switch(config)#ip igmp snooping vlan 2 limit group 300
```

38.10.11 ip igmp snooping vlan mrouter-port interface

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port interface [<*ehternet*> | <*port-channel*>] <*ifname*>

no ip igmp snooping vlan <*vlan-id*> mrouter-port interface [<*ehternet*> | <*port-channel*>] <*ifname*>

Function: Configure static mrouter port of vlan. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

ehternet: Name of Ethernet port

ifname: Name of interface

***port-channel*:** Port aggregation

Command Mode: Global mode

Default: No static mrouter port on vlan by default.

Usage Guide: When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.

Example:

```
Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/13
```

38.10.12 ip igmp snooping vlan mrpt

Command: ip igmp snooping vlan <*vlan-id*> mrpt <*value*>

no ip igmp snooping vlan <*vlan-id*> mrpt

Function: Configure this survive time of mrouter port.

Parameter: ***vlan-id*:** vlan ID, ranging between <1-4094>

***value*:** mrouter port survive period, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this vlan should be enabled previously.

Example:

```
Switch(config)#ip igmp snooping vlan 2 mrpt 100
```

38.10.13 ip igmp snooping vlan query-interval

Command: ip igmp snooping vlan <*vlan-id*> query-interval <*value*>

no ip igmp snooping vlan <*vlan-id*> query-interval

Function: Configure this query interval.

Parameter: ***vlan-id***: vlan id , ranging between <1-4094>

value: query interval, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 125s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query-interval 130
```

38.10.14 ip igmp snooping vlan query-mrsp

Command: ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>

no ip igmp snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The "**no ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value.

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: ranging between <1-25> seconds

Command Mode: Global mode

Default: 10s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query-mrsp 18
```

38.10.15 ip igmp snooping vlan query-robustness

Command: ip igmp snooping vlan <vlan-id> query-robustness <*value*>

no ip igmp snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness. The "**no ip igmp snooping vlan <vlan-id> query-robustness**" command restores to the default value.

Parameter: *vlan-id*: vlan id, ranging between <1-4094>

value: ranging between <2-10>

Command Mode: Global mode

Default: 2

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query- robustness 3
```

38.10.16 ip igmp snooping vlan report source-address

Command: ip igmp snooping vlan <*vlan-id*> report source-address <*A.B.C.D*>

no ip igmp snooping vlan <*vlan-id*> report source-address

Function: Configure forward report source-address for IGMP, the "**no ip igmp snooping vlan <*vlan-id*> report source-address**" command restores the default setting.

Parameter: *vlan-id*: vlan id range<1-4094>;

***A.B.C.D*:** IP address, can be 0.0.0.0.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream.

Example:

```
Switch (config)#ip igmp snooping vlan 2 report source-address 10.1.1.1
```

38.10.17 ip igmp snooping vlan static-group

Command: ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>

no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>]interface [ethernet | port-channel] <IFNAME>

Function: Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

A.B.C.D: the address of group or source

ethernet: Name of Ethernet port

port-channel: Port aggregation

ifname: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

```
Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/1
```

38.10.18 ip igmp snooping vlan suppression-query-time

Command: ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ip igmp snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time. The "**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value.

Parameter: ***vlan-id***: vlan id , ranging between <1-4094>

value: ranging between<1-65535> seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.

Example:

```
Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270
```

38.10.19 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the vlan number specified for displaying IGMP Snooping messages.

Command Mode: Admin Mode

Usage Guide: If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.

Example:

1. Show IGMP Snooping summary messages of the switch

```
 Switch(config)#show ip igmp snooping
Global igmp snooping status:    Enabled
L3 multicasting:                running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
---------------------------------
```

```
Switch(config)#show ip igmp snooping
Global igmp snooping status:    Enabled
L3 multicasting:                running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
---------------------------------
```

Displayed Information Explanation
Global igmp snooping status Whether the global igmp snooping switch on the switch is on
L3 multicasting whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier) which vlans on the switch is enabled with igmp snooping function, whether they are l2-general-querier

2. Display the IGMP Snooping summary messages of vlan1.

```
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1
```

```
Igmp snooping L2 general querier                    :Yes(COULD_QUERY)
Igmp snooping query-interval                        :125(s)
Igmp snooping max reponse time                       :10(s)
Igmp snooping robustness                             :2
Igmp snooping mrouter port keep-alive time           :255(s)
Igmp snooping query-suppression time                 :255(s)

IGMP Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups          Sources              Ports              Exptime   System Level
238.1.1.1       (192.168.0.1)        Ethernet1/8        00:04:14   V2
                (192.168.0.2)        Ethernet1/8        00:04:14   V2

Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/2
```

Displayed Information Explanation
Igmp snooping L2 general querier Whether the vlan enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval Query interval of the vlan
Igmp snooping max reponse time Max response time of the vlan
Igmp snooping robustness IGMP Snooping robustness configured on the vlan
Igmp snooping mrouter port keep-alive time keep-alive time of dynamic mrouter of the vlan
Igmp snooping query-suppression time Suppression timeout of vlan when as l2-general-querier
IGMP Snooping Connect Group Membership

Group membership of this vlan, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port mrouter port of the vlan, including both static and dynamic

38.11 Commands for IGMP Proxy

38.11.1 clear ip igmp proxy group

Command: clear ip igmp proxy group

Function: Delete all group records.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ip igmp proxy group
```

Relative Command: show ip igmp proxy upstream group

38.11.2 debug igmp proxy all

Command: debug igmp proxy all

no debug igmp proxy all

Function: Enable all the debugging switches of IGMP Proxy; the "**no debug igmp proxy all**" command disenables all the debugging switches.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use to enable debugging switches of IGMP Proxy, it can display IGMP packet, event, timer, mfc, which disposed in the switch.

Example:

```
Switch# debug igmp proxy all
```

38.11.3 debug igmp proxy event

Command: debug igmp proxy event

no debug igmp proxy event

Function: Enable/Disable debug switch of IGMP Proxy event.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable debugging switch if querying event information of IGMP Proxy.

Example:

```
Switch(config)#router bgp 1
```

38.11.4 debug igmp proxy mfc

Command: debug igmp proxy mfc

no debug igmp proxy mfc

Function: Enable/Disable debug switch of IGMP Proxy multicast forwarding cache.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable IGMP Proxy mfc debug switch and display multicast information created and distributed.

Example:

```
Switch# debug igmp proxy mfc
```

38.11.5 debug igmp proxy packet

Command: debug igmp proxy packet

no debug igmp proxy packet

Function: Enable/Disable debug switch of IGMP Proxy.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable the debugging switch, you can monitor the packets receiving/sending of IGMP Proxy.

Example:

```
Switch# debug igmp proxy packet
```

38.11.6 debug igmp proxy timer

Command: debug igmp proxy timer

no debug igmp proxy timer

Function: Enable/Disable each timer of IGMP Proxy.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: The command is used for enable the IGMP Proxy timer debugging switch which appointed.

Example:

```
Switch# debug ip igmp proxy timer
```

38.11.7 ip igmp proxy

Command: ip igmp proxy

no ip igmp proxy

Function: Enable the IGMP Proxy function; the "**no ip igmp proxy**" command disables this function.

Command Mode: Global Mode.

Default: The switch disables IGMP Proxy by default.

Usage Guide: Use this command to enable IGMP Proxy, and configure one upstream port and at least one downstream port under interface configuration mode if make the IGMP Proxy operate.

Example: Enable IGMP Proxy under Global Mode.

```
Switch (config)#ip igmp proxy
```

38.11.8 ip igmp proxy aggregate

Command: ip igmp proxy aggregate

no ip igmp proxy aggregate

Function: To configure non-query downstream ports to be able to aggregate the IGMP operations.

Command Mode: Global Mode.

Default: The non-query downstream ports are not to be able to aggregate the IGMP operations in default.

Usage Guide: By default non-query downstream ports cannot aggregate and redistribute the multicast messages. This command is used to enable all the downstream ports to be able to aggregate and redistribute the multicast dataflow.

Example:

```
Switch(config)#ip igmp proxy aggregate
```

38.11.9 ip igmp proxy downstream

Command: ip igmp proxy downstream

no ip igmp proxy downstream

Function: Enable the appointed IGMP Proxy downstream port function; the "**no ip igmp proxy upstream**" disables this function.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: To configure the interface to function as the downstream port of IGMP Proxy. In order to make IGMP Proxy work, at least one upstream interface should be configured. The "**no ip igmp proxy downstream**" command will disable the configuration.

Example: Enable IGMP Proxy downstream port function in interface VLAN2 under interface configuration mode.

```
Switch (config)#interface vlan 2
```

```
Switch(Config-if-Vlan2)#ip igmp proxy downstream
```

38.11.10 ip igmp proxy limit

Command: ip igmp proxy limit {group <*g_limit*> | source <*s_limit*>}

no ip igmp proxy limit

Function: To configure the maximum number of groups that upstream ports can join, and the maximum number of sources in a single group.

Parameter: *g_limit*: <1-500>, the group number limitation.

***s_limit*:** <1-500>, the source number limitation.

Command Mode: Global Mode.

Default: Most 50 groups in default, and most 40 sources in one group.

Usage Guide: If the group number limitation is exceeded, new group membership request will be rejected. This command is used to prevent malicious group membership requests.

Example:

```
Switch(config)#ip igmp proxy limit group 30 source 20
```

38.11.11 ip igmp proxy multicast-source

Command: ip igmp proxy multicast-source

no ip igmp proxy multicast-source

Function: To configure the port as downstream port for the source of multicast datagram; the no from of this command disables the configuration.

Command Mode: Interface Configuration Mode.

Default: The downstream port is not for the source of multicast datagram.

Usage Guide: When a downstream port is configured as the multicast source port, the switch will be able to receive multicast data flow from that port, and forward it to the upstream port. To make this command function, the multicast router which is connected to the upstream port of the switch, should be configured to view the multicast source from the upstream port is directly connected to the router.

Example: Enable **igmp proxy multicast-source** in downstream port VLAN1.

```
Switch (config)#interface vlan 1
```

```
Switch (Config-if-Vlan1)#ip igmp proxy multicast-source
```

38.11.12 ip igmp proxy unsolicited-report interval

Command: ip igmp proxy unsolicited-report interval <*value*>

no ip igmp proxy unsolicited-report interval

Function: To configure how often the upstream ports send out unsolicited report.

Parameter: The interval is between 1 to 5 seconds for the upstream ports send out unsolicited report.

Command Mode: Global Mode.

Default: The interval is 1 second for the upstream ports send out unsolicited report in default.

Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss. This command configures the interval for re-transmition.

Example:

```
Switch(config)#ip igmp proxy unsolicited-report interval 3
```

38.11.13 ip igmp proxy unsolicited-report robustness

Command: ip igmp proxy unsolicited-report robustness <*value*>

no ip igmp proxy unsolicited-report robustness

Function: To configure the retry times of upstream ports' sending unsolicited reports. **Parameter: *value*:** <2~10>. The retry time for upstream ports' sending unsolicited report is limited between 2 and 10.

Command Mode: Global Mode.

Default: Retry time is 2 by default.

Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss.

Example:

```
Switch(config)#ip igmp proxy unsolicited-report robustness 3
```

38.11.14 ip igmp proxy upstream

Command: ip igmp proxy upstream

no ip igmp proxy upstream

Function: Enable the appointed IGMP Proxy upstream port function. The "**no ip igmp proxy upstream**" disables this function.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: To configure the interface to function as the upstream port of IGMP Proxy. In order to make IGMP Proxy work, at least one downstream interface should be configured. The "**no ip igmp proxy upstream**" command will disable the configuration.

Example: Enable IGMP Proxy upstream port function in interface VLAN1 under interface configuration mode.

```
Switch (config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip igmp proxy upstream
```

38.11.15 ip multicast ssm

Command: ip multicast ssm range {<*1-99*>| default}

no ip multicast ssm

Function: To configure the address range for IGMP Proxy ssm multicast groups; the no form of this command will delete the ssm multicast groups.

Parameter: default: show the address range 232/8 for ssm multicast groups.

<access-list-number> is the applied access list number, range is 1-99.

Command Mode: Global Mode.

Default: The default address range is 232/8 for ssm multicast groups.

Usage Guide: The command configures the address filter for multicast group membership request. The request for the specified address ranges will be dropped. This command is also available for both the IGMP PROXY and PIM configuration. To be mentioned, this command cannot be applied with DVMRP configuration.

Example: To enable SSM configuration on the switch, and specify the address in access-list 23 as the filter address for SSM.

```
Switch(config)# access-list 23 permit host-source 224.1.1.1
```

```
Switch(config)#ip multicast ssm range 23
```

38.11.16 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure the PIM enabled port to consider all multicast source is directly connected; the no form of this command will remove the configuration.

Command Mode: Interface Configuration Mode.

Default: Disabled.

Usage Guide: Configuring the multicast source to be considered as directly connected for the PIM enabled port is used to determine the identity of DR and ORIGINATOR.

Example: To configure PIM enabled VLAN 2 as the port for BSR BORDER. For all the multicast flow from external network through VLAN 2, the switch will consider the multicast source is directly connected to the switch.

```
Switch(config)#interface vlan 2
```

```
Switch(Config-if-Vlan2)#ip pim bsr-border
```

38.11.17 show debugging igmp proxy

Command: show debugging igmp proxy

Function: Display the status of debug switch of IGMP Proxy.

Command Mode: Admin Mode.

Usage Guide: The debuging switch status of IGMP Proxy.

Example:

```
Switch(config)#show debugging igmp proxy

IGMP PROXY debugging status:
  IGMP PROXY event debugging is on
  IGMP PROXY packet debugging is on
  IGMP PROXY timer debugging is on
  IGMP PROXY mfc debugging is on
```

38.11.18 show ip igmp proxy

Command: show ip igmp Proxy

Function: Display the IGMP Proxy configuration information.

Command Mode: Admin Mode.

Usage Guide: To show configuration for **igmp proxy** about whether the **igmp proxy** is enabled globally, and whether upstream ports and downstream ports has been configured.

Example:

```
Switch(config)#show ip igmp Proxy

IGMP PROXY MRT running: Enabled
  Total active interface number: 2

Global igmp proxy configured: YES
Total configured interface number: 2
Upstream Interface configured: YES
    Upstream Interface Vlan1(2005)
Upstream Interface configured: YES
    Downstream Interface Vlan2(2006)
  --------------------------------
```

Show Information Explanation
IGMP PROXY MRT running Whether the protocol is running
Total active interface number Number of active upstream and downstream ports
Global igmp proxy configured Whether global igmp proxy is enabled
Upstream Interface configured Whether upstream port is configured
Upstream Interface Vlan The vlan which the upstream port belongs to
Upstream Interface configured Whether downstream port is configured
Downstream Interface Vlan

The vlan which the downstream port belongs to

38.11.19 show ip igmp proxy mroute

Command: show ip igmp Proxy mroute

Function: Display the status information of **igmp proxy mroute**.

Command Mode: Admin Mode.

Usage Guide: Display the status information of **igmp proxy mroute**, and information about the mrt node.

Example:

```
Switch(config)#show ip igmp proxy mroute

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 2

(1.1.1.2, 225.0.0.1)
  Local_include_olist       ..l.....................
  Local_exclude_olist       .......................
  Outgoing                  ..o.....................

(1.1.1.3, 225.0.0.1)
  Local_include_olist       ..l.....................
  Local_exclude_olist       .......................
  Outgoing                  ..o.....................
```

Show Information Explanation
Entries The counts of each item
Local_include_olist index for local include olist
Local_exclude_olist index for local exclude olist
Outgoing Final outgoing index of multicast data(S, G)

38.11.20 show ip igmp proxy upstream groups

Command: show ip igmp proxy upstream groups {A.B.C.D}

Command Mode: Admin Mode.

Usage Guide: To show the group membership information of the upstream port. If the group is not specified, information of all groups will be displayed, otherwise, only the specified will be displayed.

Example:

```
Switch(config)#show ip igmp proxy upstream groups

IGMP PROXY Connect Group Membership
Groups              Filter-mode          source
224.1.1.1           INCLUDE                192.168.1.136
226.1.1.1           *
```

Show Information Explanation
Groups IP addresses of multicast groups
Filter-mode Filter-mode of the multicast group
source Source hold by the multicast group

Chapter 39 IPv6 Multicast Protocol

39.1 Public Commands for Multicast

39.1.1 show ipv6 mroute

Command: show ipv6 mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv6 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr: show the multicast route entries relative to this source address.

Default: None

Command Mode: Admin mode and global mode

Usage Guide: None.

Example: show all entries of IPv6 multicast route table

```
Switch(config)# show ipv6 mroute
Name: Loopback, Index: 2002, State:49
Name: Vlan1, Index: 2006, State:1043
Name: Vlan11, Index: 2007, State:1043
Name: Vlan12, Index: 2008, State:1043
Name: Tunnel1, Index: 2009, State:d1
Name: Tunnel2, Index: 0, State:0
Name: pim6reg, Index: 2010, State:c1
Name: pimreg, Index: 2011, State:c1
The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1
Group          Origin              Iif        Wrong    Oif:TTL
ff2f::1        2014:1:2:3::2       Tunnel1    0        2008:1
ff3f::1        2012:1:2:3::2       NULL       4        0:0
```

Displayed information Explanation
Name the name of interface
Index the index number of interface
State the state of interface
The total matched ipmr active mfc entries The total matched active IP multicast route mfc （multicast forwarding cache） entries

unresolved ipmr entries unresolved ip multicast route entries
Group the destination address of the entries
Origin the source address of the entries
Iif ingress interface of the entries
Wrong packets received from the wrong interface
Oif egress interface of the entries
TTL the value of TTL

39.2 Commands for PIM-DM6

39.2.1 debug ipv6 pim timer sat

Command: debug ipv6 pim timer sat

no debug ipv6 pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug ipv6 pim timer sat**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

```
Switch # debug ipv6 pim timer sat
```

Remark: Other debug switches in PIM-DM are common in PIM-SM.

39.2.2 debug ipv6 pim timer srt

Command: debug ipv6 pim timer srt

no debug ipv6 pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug ipv6 pim timer srt**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail

Example:

```
Switch # debug ipv6 pim timer srt
```

Remark: Other debug switches in PIM-DM are common in PIM-SM.

39.2.3 ipv6 mroute

Command: ipv6 mroute *<X:X::X:X> <X:X::X:X> <ifname> <.ifname>*

no ipv6 mroute *<X:X::X:X> <X:X::X:X>* [*<ifname> <.ifname>*]

Function: To configure static multicast entry. This no command deletes some static multicast entries or some egress interfaces.

Parameter: *<X:X::X:X> <X:X::X:X>* are the source address and group address of multicast.

<ifname> <.ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode.

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.

Example:

```
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30
```

39.2.4 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

```
Switch(Config-if-Vlan1)#ipv6 pim bsr-border
```

39.2.5 ipv6 pim dense-mode

Command: ipv6 pim dense-mode

no ipv6 pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ipv6 pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ipv6 multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one switch. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim dense-mode

39.2.6 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, cancel and change priority value of interface DR. The same net segment border nodes vote specified router DR in this net segment through hello messages, the "no ipv6 pim dr-priority" restores default value.

Parameter: < *priority*> priority, value range from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Value range is from 0 to 4294967294, the bigger value, the more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

39.2.7 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid

no ipv6 pim exclude-genid

Function: The command make Hello message transmitted by PIM-SM exclude Genid option, the "**no ipv6 pim exclude-genid**" restores default value.

Parameter: None

Default: Hello message includes Genid option

Command Mode: Interface Configuration Mode

Usage Guide: The command is used to interactive with old Cisco IOS Version.The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello messages transmitted by switch to exclude Genid option.

```
Switch(Config-if-Vlan1)#ipv6 pim exclude-genid
```

39.2.8 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure and cancel Holdtime item value in Hello message, the value describes neighbor overtime. If it goes over the time and does not receive hello message of the neighbor, the register of the neighbor will be delete.

Parameter: <*value*> is configure time of holdtime.

Default: Define 3.5 times of Hello_interval, and default hello_interval as 30s, so default value of hello_holdtime is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If no setting, hello time will default current 3.5 times of Hello_interval. If setting hello time is less than current hello_interval, this setting will be declined. When updating hello_interval every time, hello_holdtime will be also update based on these rules below: if hello_holdtime does not be configured, or if hello_holdtime configured is less than current hello_interval, hello_holdtime will be modified to 3.5 times Hello_interval, otherwise, keeps configured value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello holdtime setting on interface vlan1 to 10.

```
Switch (config)# interface vlan1
```

```
Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10
```

39.2.9 ipv6 pim hello-interval

Command: ipv6 pim hello-interval < *interval*>

no ipv6 pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ipv6 pim hello-interval**" command restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighbor ship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime. The command can configure on IPv6 tunnel

interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure PIM-DM hello interval on interface vlan1

Switch (config)#interface vlan1
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

39.2.10 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Globally enable PIM-DM protocol; the "**no ipv6 pim multicast-routing**" command disenables PIM-DM protocol.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Global Mode

Usage Guide: Ipv6 pim can enable only after executing this command.

Example: Globally enable PIM-DM protocol

Switch (config)#ipv6 pim multicast-routing

39.2.11 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*cess-list-name*>

no ipv6 pim neighbor-filter <a*cess-list-name*>

Function: Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was broken. If no connection, the connection can be established.

Parameter: <*access-list-name*> is an applied access-list name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: If it is not necessary for partner to establish neighbor ship, the command can filter pim message of partner. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure access-list of pim neighbor on interface vlan1

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc
Switch(config)#ipv6 access-list standard myfilter

```
Switch(config_IPv6_Std-Nacl-myfilter)#permit any
```

39.2.12 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]

no ipv6 pim scope-border

Function: To configure or delete management border of PIM6.

Parameters: <*500-599*> is the ACL number for the management border.

<*acl_name*> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

```
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503
```

39.2.13 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>

no ipv6 pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The “no ipv6 pim state-refresh origination-interval” command restores default value.

Parameter: <*interval*> message transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list ltems of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

```
Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval    90
```

39.2.14 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Display PIM interface information.

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr      DR
                           Mode     Count   Prior
Vlan2        0             v2/S     0         1
      Address           : fe80::203:fff:fee3:1244
      Global Address: 2000:1:111::100
      DR                : this system
Vlan3        2             v2/S     0         1
      Address           : fe80::203:fff:fee3:1244
      Global Address: 2000:10:1:13::1
      DR                : this system
```

Displayed Information Explanations
Address Interface address
Interface Interface name
VIF index Interface index
Ver/Mode Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count The interface's neighbor count
DR Prior Dr priority
DR The interface's DR address

39.2.15 show ipv6 pim mroute dense-mode

Command: show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]

Function: Display PIM-DM message forwarding items.

Parameter: group <X:X::X:X>: displays forwarding items relevant to this multicast address

Source < X:X::X:X >: displays forwarding items relevant to this source.

Default: Do not display

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

```
Switch(config)#show ipv6 pim mroute dense-mode
IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, ff1e::15)
  Local        ..l.....................

(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local        .....................
  Pruned       .....................
  Asserted     .....................
  Outgoing     ..o.....................
```

```
Switch#
```

Displayed Information Explanations
(*, ff1e::15) (*,G) Forwaridng item
(2000:10:1:12::11, ff1e::15) (S,G) Forwarding item
RPF nbr Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx Interface located in RPF neighbor

Upstream State Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local Join Local position joins interface, the interface receives IGMP Join
Pruned PIM prunes interface, the interface receives Prune messages
Asserted Asserted state
Outgoing Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

39.2.16 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM.

Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                  Interface          Uptime/Expires     Ver   DR
Address                                                             Priority/Mode
Fe80::203:fff:fee3:1244   Vlan1              00:00:10/00:01:35  v2     1 /DR
```

```
fe80::20e:cff:fe01:facc          Vlan1                  00:00:13/00:01:32    v2        1 /
```

Displayed Information Explanations
Neighbor Address Neighbor address
Interface Neighbor interface
Uptime/Expires Running time /overtime
Ver Pim version ,v2 usually
DR Priority/Mode DR priority in the hello messages from the neighbor and if the neighbor is the interface's DR

39.2.17 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

```
Switch#show ipv6 pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable          ….
Destination              Type    Nexthop
Nexthop                                        ..Nexthop    Nexthop Metric Pref    Refcnt
                                                          Num         Addr
                                              Ifindex    Name

2000:1:111::11                                  ..S.    1              :
:                                               2004                    0          0        2
2000:1:111::100                                 .RS.    1              ::
                                               2004                    0          0        2
                          2004                  0          0        2
```

Displayed Information Explanations
Destination Destination of next item
Type N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num Nexthop number
Nexthop Addr Nexthop address
Nexthop Ifindex Nexthop interface index
Nexthop Name Nexthop name
Metric Metric Metric to nexthop
Pref Preference Route preference
Refcnt Reference count

39.3 Commands for PIM-SM6

39.3.1 clear ipv6 pim bsr rp-set

Command: clear ipv6 pim bsr rp-set *

Function: Clear all RP.

Parameters: None.

Command Mode: Admin Configuration Mode

Usage Guide: Clear all RP rapidly.

Example: Clear all RP.

```
Switch# clear ipv6 pim bsr rp-set *
```

Relative Command: show ipv6 pim bsr-router

39.3.2 debug ipv6 pim events

Command: debug ipv6 pim events

no debug ipv6 pim events

Function: Enable or Disable pim events debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable “pim events debug” switch and display events information about pim operation.

Example:

```
Switch# debug ipv6 pim events
```

39.3.3 debug ipv6 pim mfc

Command: debug ipv6 pim mfc（in|out|）

no debug ipv6 pim mfc（in|out|）

Function: Enable or Disable pim mfc debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id’s information.

Example:

```
Switch# debug ipv6 pim mfc in
```

39.3.4 debug ipv6 pim mib

Command: debug ipv6 pim mib

no ipv6 debug pim mib

Function: Enable or Disable PIM MIB debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It’s not available now and it’s for the future extension.

Example:

```
Switch# debug ipv6 pim mib
```

39.3.5 debug ipv6 pim nexthop

Command: debug ipv6 pim nexthop

no debug ipv6 pim nexthop

Function: Enable or Disable pim nexthop debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example:

```
Switch# debug ipv6 pim nexthop
```

39.3.6 debug ipv6 pim nsm

Command: debug ipv6 pim nsm

no debug ipv6 pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example:

```
Switch# debug ipv6 pim nsm
```

39.3.7 debug ipv6 pim packet

Command: debug ipv6 pim packet [in|out|]

no debug ipv6 pim packet [in|out|]

Function: Enable or Disable PIM debug switch.

Parameter: in display only received PIM packets

out display only transmitted PIM packets

none display both

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the received and transmitted PIM packets by this switch.

Example:

```
Switch# debug ipv6 pim packet in
```

39.3.8 debug ipv6 pim state

Command: debug ipv6 pim state

no debug ipv6 pim state

Function: Enable or Disable PIM debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the changing information about PIM state by this switch.

Example:

```
Switch# debug ipv6 pim state
```

39.3.9 debug ipv6 pim timer

Command: debug ipv6 pim timer

debug ipv6 pim timer assert

debug ipv6 pim timer assert at

debug ipv6 pim timer bsr bst

debug ipv6 pim timer bsr crp

debug ipv6 pim timer bsr

debug ipv6 pim timer hello ht

debug ipv6 pim timer hello nlt

debug ipv6 pim timer hello tht

debug ipv6 pim timer hello

debug ipv6 pim timer joinprune et

debug ipv6 pim timer joinprune grt

debug ipv6 pim timer joinprune jt

debug ipv6 pim timer joinprune kat

debug ipv6 pim timer joinprune ot

debug ipv6 pim timer joinprune plt

debug ipv6 pim timer joinprune ppt

debug ipv6 pim timer joinprune pt

debug ipv6 pim timer joinprune

debug ipv6 pim timer register rst

debug ipv6 pim timer register

no debug ipv6 pim timer

no debug ipv6 pim timer assert

no debug ipv6 pim timer assert at

no debug ipv6 pim timer bsr bst

no debug ipv6 pim timer bsr crp

no debug ipv6 pim timer bsr

no debug ipv6 pim timer hello ht

no debug ipv6 pim timer hello nlt

no debug ipv6 pim timer hello tht

no debug ipv6 pim timer hello

no debug ipv6 pim timer joinprune et

no debug ipv6 pim timer joinprune grt

no debug ipv6 pim timer joinprune jt

no debug ipv6 pim timer joinprune kat

no debug ipv6 pim timer joinprune ot

no debug ipv6 pim timer joinprune plt

no debug ipv6 pim timer joinprune ppt

no debug ipv6 pim timer joinprune pt

no debug ipv6 pim timer joinprune

no debug ipv6 pim timer register rst

no debug ipv6 pim timer register

no debug ipv6 pim timer

Function: Enable or Disable each PIM timer.

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable the specified timer's debug information.

Example:

```
Switch# debug ipv6 pim timer assert
```

39.3.10 ipv6 mroute

Command: ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> <*ifname*> <*.ifname*>

no ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> [<*ifname*> <*.ifname*>]

Function: To configure static multicast entry. This no command deletes some static multicast entries or some egress interfaces.

Parameter: <*X:X::X:X*> <*X:X::X:X*> are the source address and group address of multicast.

<*ifname*> <*.ifname*>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode.

Default: None.

Usage Guide: The ***<ifname>*** should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.

Example:

```
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30
```

39.3.11 ipv6 pim accept-register

Command: ipv6 pim accept-register list <*acess-list-name*>

no ipv6 pim accept-register

Function: Filter the specified multicast group.

Parameter: <*acess-list-name*> is the applying access-list name

Default: Permit the multicast registers from any sources to any groups

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets. The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP

immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured ,the default value is PERMIT..

Example: Configure the filtered register message's rule to myfilter.

```
Switch(config)#ipv6 pim accept-register list myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128
```

39.3.12 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

```
Switch(Config-if-Vlan1)#ipv6 pim bsr-border
```

39.3.13 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate {vlan <vlan_id>|tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]

no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command "**no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]**" command disables the candidate BSR.

Parameter: <vlan_id> is VLAN ID ,the value ranges from 1 to 4094;

<tunnel_id> is tunnel ID,the value ranges from 1 to 50;

<ifname> is the specified interface name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured, the default priority value is 0.

Default: This switch is not a candidate BSR router

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to

configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured, this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

```
Switch (config)# ipv6 pim bsr-candidate vlan1 30 10
```

39.3.14 ipv6 pim cisco-register-checksum

Command: ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

no ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the register packet's head length default: 8

Parameter: <*access-list name*> is the applying simple access-list.

Command Mode: Global Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

```
Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter
```

```
Switch(config)#ipv6 access-list standard myfilter
```

```
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128
```

39.3.15 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ipv6 pim dr-priority**" command restores the default value.

Parameter: <*priority*> priority, it ranges from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

```
Switch (config)# interface vlan 1
```

```
Switch(Config-if-Vlan1)ipv6 pim dr-priority 100
```

39.3.16 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid

no ipv6 pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option, the "**no ipv6 pim exclude-genid**" command restores the default value.

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the Hello packets sent by the switch do not include GenId option.

```
Switch(Config-if-Vlan1)#ipv6 pim exclude-genid
```

39.3.17 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime, if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan1's Hello Holdtime to 10s

```
Switch (config)# interface vlan1
```

```
Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10
```

39.3.18 ipv6 pim hello-interval

Command: ipv6 pim hello-interval <*interval*>

no ipv6 pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ipv6 pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan's pim-sm hello_interval.

```
Switch (config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20
```

39.3.19 ipv6 pim ignore-rp-set-priority

Command: ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: None

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, PIM usually will select according to RP priority. When this command is configured, PIM will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Configure to ignore RP priority.

```
Switch(config)#ipv6 pim ignore-rp-set-priority
```

39.3.20 ipv6 pim jp-timer

Command: ipv6 pim jp-timer <*value*>

no ipv6 pim jp-timer

Function: Configure to add JP timer. **no ipv6 pim jp-timer** restores the default value.

Parameter: <*value*> ranges from 10 to 65535

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of transmitting J/P messages to59s.

Example:

```
Switch(config)#ipv6 pim jp-timer 59
ipv6 pim multicast-routing
```

39.3.21 Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Enable PIM-SM globally. The "**no ipv6 pim multicast-routing**" command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM protocol

Command Mode: Global Mode

Usage Guide: Inspect the changing information about pim state by this switch..

Example: Enable PIM-SM globally.

```
Switch (config)#ipv6 pim multicast-routing
```

39.3.22 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <*access-list-name*>

no ipv6 pim neighbor-filter <*access-list-name*>

Function: Configure the neighbor access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: <*access-list-name*> is the applying access-list' name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1, access-list 1's default is deny. In the following example, if "permit any" is not configured, deny fe80:20e:cff:fe01:facc is the same as deny any. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan's pim neighbor access-list.

```
Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter
```

```
Switch(config)#ipv6 access-list standard myfilter
```

```
Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc
```

```
Switch(config)#ipv6 access-list standard myfilter
```

```
Switch(config_IPv6_Std-Nacl-myfilter)#permit any
```

39.3.23 ipv6 pim register-rate-limit

Command: ipv6 pim Register-rate-limit <*limit*>

no ipv6 pim Register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets, the unit is packet/second. The "**no ipv6 pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's, not the whole systems.

Parameter: <*limit*> ranges from 1 to 65535

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: Configure the speedrate of DR sending register packets.

Example: Configure the speedrate of DR sending register packets to 59 p/s.

```
Switch(config)#ipv6 pim Register-rate-limit 59
```

39.3.24 ipv6 pim register-rp-reachability

Command: ipv6 pim Register-rp-reachability

no ipv6 pim Register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration.

Parameter: None

Default: Do not check.

Command Mode: Global Mode.

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure the router to check the RP reachability before sending register packets.

```
Switch(config)# ipv6 pim Register-rp-reachability
```

39.3.25 ipv6 pim register-source

Command: ipv6 pim register-source {<*source-address*> |<*ifname*>|vlan <*vlan-id*>}

no ipv6 pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter: <*ifname*> is the interface name that will be the register packets source.

<*source-address*> is the interface address will be the register packets source. In the format of hex without prefix length.

<*vlan-id*> is the VLAN ID.

Default: Do not check.

Command Mode: Global Mode

Usage Guide: The "**no ipv6 pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address of the sent register packets to vlan1's address

```
Switch(config)# ipv6 pim register-source Vlan1
```

39.3.26 ipv6 pim register-suppression

Command: ipv6 pim register-suppression <*value*>

no ipv6 pim register-suppression

Function: This command is to configure the value of register suppression timer, the unit is second.

Parameter: <*value*> is the timer's value, it ranges from 10 to 65535s.

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR, it's the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value. The "**no ipv6 pim register-suppression**" command restores the default value.

Example: Configure the value of register suppression timer to 30s.

```
Switch(config)# ipv6 pim register-suppression 30
```

39.3.27 ipv6 pim rp-address

Command: ipv6 pim rp-address <*rp-address*> [<*group-range*>]

no ipv6 pim rp-address <*rp-address*> [all|<*group-range*>]

Function: This command is to configure static RP globally or in a multicast address range. The "**no ipv6 pim rp-address**" command cancels static RP.

Parameter: <*rp-address*> is the RP address, the format is **X:X::X:X** ,**ipv6** address

<*group-range*> is the expected RP, the format is **X:X::X:X/M, ipv6** address and prefix length all the ranges

Default: This switch is not a RP static router

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range.

Example: Configure 2000:112::8 as RP address globally.

```
Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64
```

39.3.28 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate{vlan<vlan-id> |loopback<index> |<ifname>}[<group range>] [<priority>]

no ipv6 pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ipv6 pim rp-candiate**" command cancels the candidate RP.

Parameter: <vlan_id> is VLAN ID；

<index> is Loopback interface index;

<*ifname*> is the name of the interface;

<*group range*> is the group range of the candidate RP,the format is **X:X::X:X/M**, **ipv6** address and prefix length;

<*priority*> is the RP selection priority, ranges from 0 to 255, the default value is 192, the

lower value has more priority

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. Only this command is configured, this switch is the RP candidate router

Example: Configure vlan1 as the sending interface of candidate RP announce messages

```
Switch (config)# ipv6 pim rp-candidate vlan1 100
```

39.3.29 ipv6 pim rp-register-kat

Command: ipv6 pim rp-register-kat <*vaule*>

no ipv6 pim rp-register-kat

Function: This command is to configure the KAT(KeepAlive Timer)value of the RP(S,G)items, the unit is second. The "**no ipv6 pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value, ranges from 1 to 65535s

Default: 185s

Command Mode: Global Mode

Usage Guide: Configure rp-register-kat interval to 30s.

Example:

```
Switch(config)# ipv6 pim rp-register-kat 30
```

39.3.30 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]

no ipv6 pim scope-border

Function: To configure or delete management border of PIM6.

Parameters: <*500-599*> is the ACL number for the management border.

<*acl_name*> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the management border and the ACL for the IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

```
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503
```

39.3.31 ipv6 pim sparse-mode

Command: ipv6 pim sparse-mode [passive]

no ipv6 pim sparse-mode [passive]

Function: Enable PIM-SM on the interface. **no ipv6 pim sparse-mode [passive]** disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable MLD(reveice and transmit MLD packets).

Default: Disabled PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-SM on the interface vlan1.

```
Switch (config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
```

39.3.32 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router

Function: Display BSR address.

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Example:

```
Switch#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2000:1:111::100 (?)
  Uptime:      00:16:00, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:10
  Role: Candidate BSR
  State: Elected BSR
Next Cand_RP_advertisement in 00:00:10
  RP: 2000:1:111::100(Vlan2)
```

Displayed Information Explanations
BSR address Bsr-router Address
Priority Bsr-router Priority
Hash mask length Bsr-router hash mask length
State The current state of this candidate BSR, Elected BSR is selected BSR

39.3.33 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Display PIM interface information.

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                           Mode     Count    Prior
Vlan2        0             v2/S     0          1
      Address            : fe80::203:fff:fee3:1244
      Global Address: 2000:1:111::100
      DR                 : this system
Vlan3        2             v2/S     0          1
      Address            : fe80::203:fff:fee3:1244
      Global Address: 2000:10:1:13::1
      DR                 : this system
```

Displayed Information Explanations
Address Interface address
Interface Interface name
VIF index Interface index
Ver/Mode Pim version and mode, usually v2,sparse mode displays S,dense mode displays D
Nbr Count The interface's neighbor count
DR Prior Dr priority
DR The interface's DR address

39.3.34 show ipv6 pim mroute sparse-mode

Command: show ipv6 pim mroute sparse-mode

Function: Display the multicast route table of PIM-SM.

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example:

```
Switch#show ipv6 pim mr    group ff1e::15
IPv6 Multicast Routing Table
  (*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
  (*, ff1e::15)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
  Local        ..l.....................
  Joined       .....................
  Asserted     .....................
FCR:
  (2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
  Local        .....................
  Joined       .....................
  Asserted     .....................
  Outgoing     ..o.....................
  (2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
  Pruned       .....................
  Outgoing     ..o.....................
```

Displayed Information Explanations
Entries The counts of each item
RP Share tree's RP address
RPF nbr RP direction or upneighbor of source direction
RPF idx RPF nbr interface
Upstream State Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local Local join interface, this interface receive IGMPJoin
Joined PIM join interface, this interface receive J/P messages
Asserted Asserted state
Outgoing Final outgoing of multicast data

39.3.35 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM.

Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                Interface       Uptime/Expires    Ver   DR
Address                                                         Priority/Mode
Fe80::203:fff:fee3:1244 Vlan1           00:00:10/00:01:35 v2      1 /DR
fe80::20e:cff:fe01:facc Vlan1           00:00:13/00:01:32 v2      1 /
```

Displayed Information Explanations
Neighbor Address Neighbor address
Interface Neighbor interface
Uptime/Expires Running time /overtime
Ver Pim version ,v2 usually
DR Priority/Mode DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

39.3.36 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

```
Switch#show ipv6 pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable          ….
Destination             Type    Nexthop
Nexthop                                        ..Nexthop    Nexthop Metric Pref    Refcnt
                                                        Num          Addr
```

```
                                    Ifindex    Name
------------------------------------------------------------------------------
2000:1:111::11                          ..S.  1             :
:                                       2004                0       0       2


2000:1:111::100                         .RS.  1             ::
                                        2004                0       0       2
                          2004          0       0       2
```

Displayed Information Explanations
Destination Destination of next item
Type N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num Nexthop number
Nexthop Addr Nexthop address
Nexthop Ifindex Nexthop interface index
Nexthop Name Nexthop name
Metric Metric Metric to nexthop
Pref Preference Route preference
Refcnt Reference count

39.3.37 show ipv6 pim rp-hash

Command: show ipv6 pim rp-hash X:X::X:X

Function: Display the RP address of group X:X::X:X's merge point.

Parameter: Group address

Default: None

Command Mode: Any Mode

Usage Guide: Display the RP address corresponding to the specified group address.

Example:

```
Switch#show ipv6 pim rp-hash ff1e::15
    RP: 2000:1:111::100
    Info source: 2000:1:111::100, via bootstrap
```

Displayed Information Explanations
RP Queried group'sRP
Info source The source of Bootstrap information

39.3.38 show ipv6 pim rp mapping

Command: show ipv6 pim rp mapping

Function: Display Group-to-RP Mapping and RP.

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the current RP and mapping relationship.

Example:

```
Switch#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2000:1:111::100
    Info source: 2000:1:111::100, via bootstrap, priority 192
        Uptime: 00:10:24, expires: 00:02:06
Group(s): ff00::/8, Static
    RP: 2000:1:111::100
        Uptime: 00:11:01
```

Displayed Information Explanations
Group(s) Group address range of RP
Info source Source of Bootstrap messages
Priority Priority of Bootstrap messages

39.4 Commands for ANYCAST RP v6

39.4.1 debug ipv6 pim anycast-rp

Command: debug ipv6 pim anycast-rp

no debug ipv6 pim anycast-rp

Function: Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.

Command Mode: Admin Mode.

Default: The debug switch of ANYCAST RP is disabled by default.

Usage Guide: This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example:

```
Switch#debug ipv6 pim anycast-rp
```

39.4.2 ipv6 pim anycast-rp

Command: ipv6 pim anycast-rp

no ipv6 pim anycast-rp

Function: Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.

Command Mode: Global Configuration Mode.

Default: The switch will not enable the ANYCAST RP by default.

Usage Guide: This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.

Example: Enable ANYCAST RP in global configuration mode.

```
Switch(config)#ipv6 pim anycast-rp
```

39.4.3 ipv6 pim anycast-rp

Command: ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>

no ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>

Function: Configure ANYCAST RP address（ARA）and the unicast addresses of other RP communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.

Parameters: *anycast-rp-addr*: RP address, the current absence of the candidate interface in accordance with the address is allowed.

***other-rp-addr*:** The unicast address of other RP communicating with this router(as a RP).

Command Mode: Global Configuration Mode.

Default: There is no configuration by default.

Usage Guide:

1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.

2. Configure the other-rp-address of other RPs communicating with this router (as a RP). The unicast address identifies other RP, and is used to communicate with the local router.

3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.

4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received, it should be forwarded to all of these other RP one by one.

Example: Configure other-rp-address in global configuration mode.

```
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2
```

39.4.4 ipv6 pim anycast-rp self-rp-address

Command: ipv6 pim anycast-rp self-rp-address <*self-rp-addr*>

no ipv6 pim anycast-rp self-rp-address

Function: Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.

Parameters: *self-rp-addr*: The unicast address used by this router (as a RP) to communicate with other RP.

Command Mode: Global Configuration Mode.

Default: No self-rp-address is configured by default.

Usage Guide:

1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.

2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a

register-stop message, whose destination address is the source address of the register message.

3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.

Example: Configure the self-rp-address of this router in global configuration mode.

```
Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1
```

39.4.5 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A:B::C:D*>] [<*priority*>]

no ipv6 pim rp-candidate

Function: Add a Loopback interface as a RP candidate interface based on the original PIM6-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.

Parameters: *index*: Loopback interface index, whose range is <1-1024>.

***vlan-id*:** the Vlan ID.

***ifname*:** the specified name of the interface.

A:B::C:D/M: the ip prefix and mask.

***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.

Command Mode: Global Configuration Mode.

Default Setting: No RP interface is configured by default.

Usage Guide: In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ipv6 pim rp-candidate” command can be used to cancel the RP candidate.

Example: Configure Loopback1 interface as the RP candidate interface in global configuration mode.

```
Switch(config)# ipv6 pim rp-candidate loopback1
```

39.4.6 show debugging ipv6 pim

Command: show debugging ipv6 pim

Command Mode: Admin and Configuration Mode.

Usage Guide: The current state of ANYCAST RP debug switch.

Example:

```
Switch(config)#show debugging ipv6 pim

Debugging status:
   PIM anycast-rp debugging is on
```

39.4.7 show ipv6 pim anycast-rp first-hop

Command: show ipv6 pim anycast-rp first-hop

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.

Example:

```
Switch(config)#show ipv6 pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (2000:1:111::2, ffle::1)
  Local        .l.....................
```

Display Explanation
Entries The number of all kinds of entries.
INCLUDE The mrt information created in the first hop RP.

39.4.8 show ipv6 pim anycast-rp non-first-hop

Command: show ipv6 pim anycast-rp non-first-hop

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.

Example:

```
Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0
```

```
INCLUDE (2002:1:111::2, ffle::2)
 Local        .l.....
```

Display Explanation
Entries The number of all kinds of entries.
INCLUDE The mrt information created in the first hop RP.

39.4.9 show ipv6 pim anycast-rp status

Command: show ipv6 pim anycast-rp status

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured ANYCAST RP set.

Example:

```
Switch(config)#show ipv6 pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:2004::2

anycast-rp address: 2000:1:111::2
      other rp unicast rp address: 2002::1
      other rp unicast rp address: 2005::1

anycast-rp address: 2003::1
      other rp unicast rp address: 2002::2
 --------------------------------
```

Display Explanation
anycast-rp: Whether the ANYCAST RP switch is globally enabled.

self-rp-address: The configured self-rp-address.
anycast-rp address: The configured anycast-rp-address.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.
anycast-rp address: The configured anycast-rp-address*.
other rp unicast rp address: The configured other RP communication addresses in accordance with the above anycast-rp-address.

39.5 Commands for PIM-SSM6

39.5.1 ipv6 pim ssm

Command: ipv6 pim ssm {default|range <*access-list-name* >}

no ipv6 pim ssm

Function: Configure the range of pim ssm multicast address. The "**no ipv6 pim ssm**" command deletes configured pim ssm multicast group.

Parameter: default: indicates the default range of pim ssm multicast group is ff3x::/32.

<access-list-number > is the name of applying access-list.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ipv6 pim multicasting succeed.

3. Access-list only can use the lists created by ipv6 access-list.

4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ipv6 pim ssm can release the bondage.

5. If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

```
Switch (config)#ipv6 pim ssm range 23
```

```
Switch(config)#ipv6 access-list standard myfilter
```

```
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::/48
```

39.6 Commands for IPv6 DCSCM

39.6.1 ipv6 access-list(ipv6 multicast source control)

Command: ipv6 access-list *<8000-8099>* {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

no ipv6 access-list *<8000-8099>* {deny|permit} {{<*source/M*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

Function: Configure IPv6 source control multicast access list, the no operation of this command is used to delete the access list.

Parameters: *<8000-8099>*: The source control access list number.

{deny|permit}: Deny or permit.

***<source/M>*:** The multicast source address and the length of mask.

***<source-host-ip>*:** The multicast host address.

***<destination/M>*:** The multicast destination address and the length of mask.

***<destination-host-ip>*:** The multicast destination host addresses.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: IPv6 multicast source control entries control the ACL it uses with ACL number 8000-8099, this command is used to configure such ACL. IPv6 multicast source control ACL only needs to configure the source IPv6 address and destination IPv6 address (that is the group IPv6 addresses)which are to be controlled, the configuration adopts a method similar to other ACLs, which can either be an address range configured by the length of mask, or a specified host address or all addresses. Pay attention to that: for group IPv6 addresses, the “all addresses” mentioned here is ff:/8.

Example:

```
Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64
```

39.6.2 ipv6 access-list(multicast destination control)

Command: ipv6 access-list *<9000-10999>* {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

no ipv6 access-list *<9000-10999>* {deny|permit} {{<*source/M*> }|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}

Function: Configure IPv6 destination control multicast access list, the no operation of this command is used to delete the access list.

Parameters: <9000-10999>: The source control access list number.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and the length of mask.

<source-host-ip>: Multicast source host address.

<destination/M>: Multicast destination address and the length of mask.

<destination-host-ip>: Multicast destination host address.

Default: None.

Command Mode: Global Configuration Mode.

Usage Guide: IPv6 multicast destination control entries control the ACL it uses with ACL number 9000-10999, this command is used to configure such ACL. IPv6 multicast source control ACL only needs to configure the source IPv6 address and destination IPv6 address (that is the group IPV6 addresses) , the configuration adopts a method similar to other ACLs, which can either be a address range configured by the length of mask, or a specified host address or all addresses Which are to be controlled. Pay attention to that, for group IPV6 addresses, the “all addresses” mentioned here is ff:/8.

Example:

```
Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ff1e::1/64
```

39.6.3 ipv6 multicast destination-control access-group

Command: ipv6 multicast destination-control access-group <*9000-10999*>

no ipv6 multicast destination-control access-group <*9000-10999*>

Function: Configure the IPv6 multicast destination control access list used by the port, the no operation of the command will delete this configuration.

Parameters: <*9000-10999*>: The destination control access list number.

Default: Not configured.

Command Mode: Port Configuration Mode.

Usage Guide: This command can only take effect when the IPv6 multicast destination control is globally enabled, after configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or it can not be added.

Example:

```
switch(config)#inter ethernet 1/4
switch(Config-If-Ethernet1/4)#ipv6 multicast destination-control access-group 9000
switch(Config-If-Ethernet1/4)#
```

39.6.4 ipv6 multicast destination-control access-group (sip)

Command: ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>*

no ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>*

Function: Configure multicast destination-control access-list used on specified net segment, the "**no ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>***"command deletes this configuration.

Parameter: *<IPADDRESS/M>*: IP address and mask length;

***<9000-10999>*:** Destination control access-list number.

Default: None.

Command Mode: Global Mode.

Usage Guide: The command is only working under global IPv6 multicast destination-control enabled, after configuring the command, if MLD-SPOOPING or MLD is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted MLD-REPORT, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in **show ipv6 mld groups detail** has been established before executing the command, it needs to execute **clear ipv6 mld group** command to clear relevant groups in admin mode.

Example:

```
Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000
```

39.6.5 ipv6 multicast destination-control access-group (vmac)

Command: ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>*

no ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>*

Function: Configure the IPv6 multicast destination access list used by the specified vlan-mac, the no operation of this command will delete this configuration.

Parameters: *<1-4094>*: VLAN-ID;

***<macaddr>*:** The source MAC address sending of the MLD-REPORT, the format of which is"xx-xx-xx-xx-xx-xx".

***<9000-10999>*:** Destination access list number.

Default: Not configured.

Command Mode: Global Configuration Mode.

Usage Guide: This command can only take effect when the IPv6 multicast destination control is globally enabled, after configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or it can not be added.

Example:

```
switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000
```

39.6.6 ipv6 multicast policy

Command: ipv6 multicast policy <*IPADDRSRC/M*> <*IPADDRGRP/M*> cos <*priority*>

no ipv6 multicast policy <*IPADDRSRC/M*> <*IPADDRGRP/M*> cos

Function: Configure IPv6 policy multicast, the no operation of this command is to cancel the policy multicast of IPv6.

Parameters: <*IPADDRSRC/M*>: The source address and the length of the mask of IPv6 multicast.

<*IPADDRGRP/M*>: The multicast address of IPv6 and the length of mask of multicast address

<*priority*>: The specified priority, the range of which is <0-7>.

Default: Not configured.

Command Mode: Global Configuration Mode.

Usage Guide: Using this command to configure can change the priority of the multicast data which is confined by the act of matching of this switch to a specified value, and set the TOS to the same value simultaneously. Please pay attention to that, for the messages sent in UNTAG mode, their priority will not be changed.

Example:

```
Switch(config)#ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4
```

39.6.7 ipv6 multicast source-control

Command: ipv6 multicast source-control

no ipv6 multicast source-control

Function: Configure to globally enable IPv6 multicast source control, the no operation of this command is to recover and globally disable the IPv6 multicast source control.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only when the IPv6 multicast source control is enabled globally, the source control access list can be applied to ports. After configuring this command, the IPv6 multicast data received by all the ports will be dropped by the switch if there is no matched multicast source control entry, that it only the multicast data matched as PERMIT can be received and forwarded.

Example:

```
Switch(config)#ipv6 multicast source-control
```

39.6.8 ipv6 multicast source-control access-group

Command: ipv6 multicast source-control access-group <*8000-8099*>

no ipv6 multicast source-control access-group <*8000-8099*>

Function: Configure the multicast source control access list used by the port, the no operation of this command is used to delete the configuration.

Parameters: <*8000-8099*>: Source control access list number.

Default: Not configured.

Command Mode: Port Configuration Mode.

Usage Guide: This command can only be successfully configured when the IPv6 multicast source control is globally enabled, after configuring this command, all the IPv6 multicast messages entering from the port will be matched according to the configured access list, only when the message is matched as permit, can it be received and forwarded, or it will be dropped.

Example:

```
switch(config)#inter ethernet 1/4
switch(Config-If-Ethernet1/4)#ipv6 multicast source-control access-group 8000
```

39.6.9 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPv4 and IPv6 multicast destination control, after configuring this command, IPv4 and IPv6 multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPv4 and IPv6 multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only after globally enabling the multicast destination control, the other destination control configuration can take effect, the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING, MLD-SNOOPING and IGMP, MLD will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT and MLD-REPORT.

Example:

```
switch(config)# multicast destination-control
```

39.6.10 show ipv6 multicast destination-control

Command: show ipv6 multicast destination-control [detail]

show ipv6 multicast destination-control interface <*Interfacename*> [detail]

show ipv6 multicast destination-control host-address <*ipv6addr*> [detail]

show ipv6 multicast destination-control <*vlan-id*> <*mac*> [detail]

Function: Display IPv6 multicast destination control configuration.

Parameters: detail: Whether to display detailed information.

***<Interfacename>*:** Interface name.

***<ipv6addr>*:** IPv6 address.

***<vlan-id>* :** VLAN ID.

***<mac>*:** MAC address.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured multicast destination control rules, if including the detail option, it will also display the details of the access-list in use.

Example:

```
switch(config)#show ipv6 multicast destination-control
ipv6 multicast destination-control is enabled
ipv6 multicast destination-control 2003::1/64 access-group 9003
ipv6 multicast destination-control 1 00-03-05-07-09-11 access-group 9001
multicast destination-control access-group 6000 used on interface Ethernet1/13
```

```
switch(config)#
```

39.6.11 show ipv6 multicast destination-control access-list

Command: show ip multicast destination-control access-list

show ip multicast destination-control access-list *<9000-10999>*

Function: Display the configured IPv6 destination control multicast access list.

Parameters: *<9000-10099>*: Access list number.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured IPv6 destination control multicast access list.

Example:

```
switch# sh ipv6 multicast destination-control acc
 ipv6 access-list 9000 permit 2003::2/64 ff1e::3/64
 ipv6 access-list 9000 deny 2008::1/64 ff1e::1/64
 ipv6 access-list 9000 permit any-source any-destination
 ipv6 access-list 9001 deny any-source host-destination ff1a::1
 ipv6 access-list 9001 permit any-source any-destination
```

39.6.12 show ipv6 multicast policy

Command: show ipv6 multicast policy

Function: Display the configured IPv6 multicast policy.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured IPv6 multicast policy.

Example:

```
switch#show ipv6 multicast policy
```

```
ipv6 multicast-policy 2003::2/64 ff1e::3/64 cos 5
```

39.6.13 show ipv6 multicast source-control

Command: show ipv6 multicast source-control [detail]

show ipv6 multicast source-control interface <*Interfacename*> [detail]

Function: Display IPv6 multicast source control configuration.

Parameters: *detail*: whether to display detailed information.

***<Interfacename>*:** Port name.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured multicast source control rules, if including the detail option, it will also display the details of the access-list in use.

Example:

```
Switch#show ipv6 multicast source-control detail
Ipv6 multicast source-control is enabled
Interface Ethernet 1/1 use multicast source control access-list 8000
  ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
  ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64
  ipv6 access-list 8000 permit any-source any-destination
```

39.6.14 show ipv6 multicast source-control access-list

Command: show ipv6 multicast source-control access-list

show ipv6 multicast source-control access-list <*8000-8099*>

Function: Display the configured IPv6 source control multicast access list.

Parameters: <*8000-8099*>: Access list number.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Use this command to display the configured source control multicast access list.

Example:

```
switch#sh ipv6 multicast source-control access-list
  ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
  ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64
```

39.7 Commands for MLD

39.7.1 clear ipv6 mld group

Command: clear ipv6 mld group [X:X::X:X | IFNAME]

Function: Delete the group record of the specific group or interface.

Parameters: X:X::X:X the specific group address; IFNAME the specific interface address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ipv6 mld group
```

Relative Command: show ipv6 mld group

39.7.2 debug ipv6 mld events

Command: debug ipv6 mld events

no debug ipv6 mld events

Function: Enable the debug switch that displays MLD events. The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: This switch can be enabled to get MLD events information.

Example:

Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present

```
Switch# debug ipv6 mld events
```

```
Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3
1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003
1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present
```

39.7.3 debug ipv6 mld packet

Command: debug ipv6 mld packet

no debug ipv6 mld packet

Function: Enable the debug switch that displays MLD packets. The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD packets information.

Example:

```
Switch# deb ipv6 mld packet
```

```
Switch#1970/01/01 07:33:12 IMI: Recv MLD packet
1970/01/01 07:33:12 IMI:    Type: Listener Report (131)
1970/01/01 07:33:12 IMI:    Code: 0
1970/01/01 07:33:12 IMI:    Checksum: 3b7a
1970/01/01 07:33:12 IMI:    Max Resp Delay: 0
```

```
1970/01/01 07:33:12 IMI:    Reserved: 0
1970/01/01 07:33:12 IMI:    Multicast Address: ff1e::1:3
1970/01/01 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3
1970/01/01 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003
1970/01/01 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --> Listeners Present
```

39.7.4 ipv6 mld access-group

Command: ipv6 mld access-group {*<acl_name>*}

no ipv6 mld access-group

Function: Configure the access control of the interface to MLD groups; the "**no ipv6 mld access-group**" command stops the access control.

Parameter: *<acl-name>* is the name of IPv6 access-list

Default: no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure the interface to filter MLD groups, allow or deny some group's join.

Example: Configure the interface vlan2 to accept group FF1E::1:0/112 and deny others

```
Switch (config)# ipv6 access-list aclv6 permit FF1E::1:0/112
Switch (config)# ipv6 access-list aclv6 deny any
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld access-group aclv6
```

39.7.5 ipv6 mld immediate-leave

Command: ipv6 mld immediate-leave group-list {*<acl-name>*}

no ipv6 mld immediate-leave

Function: Configure MLD to work in the immediate leave mode, that's when the host sends a membership qualification report that equals to leave a group, the router doesn't send query and consider there is no this group's member in the subnet. The **"no ipv6 mld immediate-leave**" command cancels the immediate leave mode.

Parameter: *<acl-name>* is the name of IPv6 access-list

Default: Do not configure immediate-leave group

Command Mode: Interface Configuration Mode

Usage Guide: This command is used only when there is only one host in the subnet.

Example: Configure access-list"aclv6"as immediate leave mode.

```
Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6
```

39.7.6 ipv6 mld join-group

Command: ipv6 mld join-group *<address>*

no ipv6 mld join-group <address>

Function: Configure the interface to join in certain multicast group; the "**no ipv6 mld join-group <address>**" command cancels joining certain multicast group.

Parameter: *<address>* is a valid IPv6 multicast address

Default: No multicast group joined by factory default

Command Mode: Interface Configuration Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in.

Example: Join the interface vlan2 in multicast group with multicast address of ff1e::1:3.

Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3

39.7.7 ipv6 mld join-group mode source

Command: ipv6 mld join-group *<X:X::X:X>* mode *<include|exclude>* source *<.X:X::X:X>*

no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>

Function: Configure the sources of certain multicast group which the interface join in. Note: because of the client group has got only INLCUDE and EXCLUDE modes, if the source mode is not in accordance with current mode configured, the group mode will be changed and the original sources of the other modes configured will be cleared permanently; the "no" form of this command cancels joining certain group.

Parameter: *<X:X::X:X>* is a valid IPv6 multicast address

***<include|exclude>*:** joining mode

***<.X:X::X:X>*:** source list, configure several sources is allowed.

Default: No multicast group to be joined by factory default

Command Mode: Interface Configuration Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in. As for sources with mode same as the original one, the source will be added, while for those with different modes, the original sources will be cleared.

Example:

Join vlan2 in multicast group with multicast address of ff1e::1:3, with sources 2003::1 and 2003::2 in INCLUDE mode.

Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source 2003::1 2003::2

39.7.8 ipv6 mld last-member-query-interval

Command: ipv6 mld last-member-query-interval *<interval>*

no ipv6 mld last-member-query-interval

Function: Configure the interface's sending interval of querying specific group. The "**no ipv6 mld last-member-query-interval**" command cancels the manually configured value and restores the default value.

Parameter: <*interval*> is the interval of querying specific group, it ranges from 1000 to 25500ms. It's the integer times of 1000ms. If it's not the integer times of 1000ms, the system will convert it to the integer times of 1000ms.

Default: 1000ms.

Command Mode: Interface Configuration Mode

Example: Configure the interface vlan1's MLD last-member-query-interval as 2000.

```
Router(config)#int vlan 1
Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000
```

39.7.9 ipv6 mld limit

Command:ipv6 mld limit <*state-count*>

no ipv6 mld limit

Function: Configure the MLD state count limit of the interface; the "**no ipv6 mld limit**" command restores the manually configured value to default value.

Parameter: <*state-count*>:max MLD state the interface maintains, the valid range is 1-5000.

Default: 400 by default

Command Mode: Interface Configuration Mode

Usage Guide: When max state-count is configured, the number of the state the interface saves will only upper to the state-count limit; and when the max state-count is reached, the later new member qualification report received will be ignored. If some MLD group state has already been saved before this command configured, the original states will be removed and the MLD general query will be sent to collect group member qualification reports no more than the max state-count.

Example: Set the MLD state-count limit of the interface vlan2 to 4000.

```
Switch(config)#interface vlan2
Switch(Config-if-Vlan2)#ipv6 mld limit 4000
```

39.7.10 ipv6 mld query-interval

Command: ipv6 mld query-interval <*time_val*>

no ipv6 mld query-interval

Function: Configure the interval of the periodically sent MLD host-query messages; the "**no ipv6 mld query-interval**" command restores the default value.

Parameter: <*time_val*> is the interval of the periodically sent MLD host-query messages; it ranges from 0 to 65535s

Default: Intrerval of periodically transmitted MLD query message is 125s.

Command Mode: Interface Configuration Mode

Usage Guide: When a interface enables a kind of multicast protocol, it will send MLD host-query messages periodically. This command is used to configure the query period.

Example: Configure the interval of the periodically sent MLD host-query messages to 10s.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query-interval 10

39.7.11 ipv6 mld query-max-response-time

Command: ipv6 mld query-max-response-time <*time_val*>

no ipv6 mld query- max-response-time

Function: Configure the maximum of the response time of MLD queries; the "**no ipv6 mld query-max-response-time**" command restores the default value.

Parameter: <*time_val*> is the maximum of the response time of MLD queries, it ranges from 1 to 25s.

Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: When the switch receives a query message, the host will set a timer to each multicast group. The timer's value is between 0 to the maximum response time. When any one of the timers decreases to 0, the host will group member announce messages. Configuring the maximum response time reasonablely, the host can swiftly response to the query messages and the router can also get the group members' existing states quickly.

Example: Configure the maximum response time of MLD queries to 20s.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query- max-response-time 20

39.7.12 ipv6 mld query-timeout

Command: ipv6 mld query-timeout <*time_val*>

no ipv6 mld query-timeout

Function: Configure the interface's timeout of MLD queries; the "**no ipv6 mld query-timeout**" command restores the default value.

Parameter: <*time_val*> is the timeout of MLD queries, it ranges from 60 to 300s

Default: 255s

Command Mode: Interface Configuration Mode

Usage Guide: In the share network, when there are more switches that run MLD, one switch will be selected as the querying host and others set a timer to inspect the querying host's state. If no querying packet is received when the timeout is over, a switch will be reselected as the querying host.

Example: Configure the interface's timeout of MLD queries to 100s.

Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query-timeout 100

39.7.13 ipv6 mld static-group

Command: ipv6 mld static-group <group_address> [source <source_address>]

no ipv6 mld static-group <group_address> [source <source_address>]

Function: Configure certain static group or static source on the interface. The “no” form of this command cancels certain previously configured static group or static source.

Parameter:<group_address> is a valid IPv6 multicast address;<source_address> is a valid IPv6 unicast address.

Default: No static group or static source is configured on the interface by factory default.

Command Mode: Interface Configuration Mode

Usage Guide: The valid range of the static group multicast address configured by the interface is the dynamic multicast address specified by the IPv6 protocol. Once the interface configures static group or static source for the multicast address, no matter whether there is membership qualification report of this group or source in the subnet, MLD protocol will consider that the group or source exist. Note: the configured static source is the source to be forwarded.

Example: Configure an MLD static-group ff1e::1:3 on interface vlan2.

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 Configure a static source 2001::1 of the group ff1e::1:3 on interface vlan2
Switch(config)#int vlan2
Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

39.7.14 ipv6 mld version

Command: ipv6 mld version <*version_no*>

no ipv6 mld version

Function: Configure the version of the MLD protocol running on the interface; the “**no ipv6 mld version**” command restores the manually configured version to the default one.

Parameter: <*version_no*> is the version number of the MLD protocol, with a valid range of 1-2.

Default: 2 by default

Command Mode: Interface Configuration Mode

Usage Guide: While there is routers still not upgraded to version 2 of MLD protocol on the subnet connected, the interface should be configured to corresponding version.

Example: Configure the MLD version to 2.

Switch(config)#ipv6 mld version 2
Switch(config)#

39.7.15 show ipv6 mld groups

Command: show ipv6 mld groups [{*<ifname | group_addr>*}]

Function: Display the MLD group information.

Parameter: ***<ifname>*** is the name of the interface. Display the MLD group information. ***<group_addr>*** is the group address. Display the specified group information.

Default: Do not display

Command Mode: Admin Mode

Example:

```
Switch#sh ipv6 mld group
MLD Connected Group Membership
Group Address                    Interface            Uptime    Expires
ff1e::1:3                        Vlan1                00:00:16  00:03:14

Switch#
```

Displayed Information Explanations
Group Address Multicast group IP address
Interface The interface of multicast group
Uptime The existing time of the multicast group
Expires The left time to overtime

39.7.16 show ipv6 mld interface

Command: show ipv6 mld interface [*<ifname>*]

Function: Display the relevant MLD information of an interface.

Parameter: ***<ifname>*** is the name of the interface. Display the MLD information of a specific interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display the MLD information of the Ethernet Interface vlan1

```
Switch#show ipv6 mld interface Vlan1
Interface Vlan1(2003)
  Index 2003
  Internet address is fe80::203:fff:fe01:e4a
```

```
MLD querier
MLD query interval is 100 seconds
MLD querier timeout is 205 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1000 ms
Group membership interval is 210 seconds
MLD is enabled on interface
```

39.7.17 show ipv6 mld join-group

Command: show ipv6 mld join-group

show ipv6 mld join-group interface {vlan <*vlan_id*>|<*ifname*>}

Function: Display the join-group messages on the interfaces.

Parameters: <ifname> is the name of the interface, which means to display MLD information on the specified interface.

Default: Do not display

Command Mode: Admin and Configuration Mode.

Example: Display the MLD information on Ethernet interfaces in vlan2.

```
Switch#show ipv6 mld join-groups interface Vlan2
Mld join group information:
INTERFACE: Vlan2
HOST VERSION: 2
MULTICAST ADDRESS: ff1e:: 1:3
GROUP STATE: EXCLUDE
SOURCE ADDRESS: 2003::1 mode: EXCLUDE
SOURCE ADDRESS: 2003::2 mode: EXCLUDE
SOURCE ADDRESS: 2003::6 mode: EXCLUDE
SOURCE ADDRESS: 2003::9 mode: EXCLUDE
```

39.8 Commands for MLD Snooping Configuration

39.8.1 clear ipv6 mld snooping vlan

Command: clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]

Function: Delete the group record of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; X:X::X:X the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

```
Switch#clear ipv6 mld snooping vlan 1 groups
```

Relative Command: show ipv6 mld snooping vlan <1-4094>

39.8.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Command: clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME|IFNAME]

Function: Delete the mrouter port of the specific VLAN.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete the mrouter port in vlan 1.

```
Switch# clear ipv6 mld snooping vlan 1 mrouter-port
```

Relative Command: show ipv6 mld snooping mrouter-port

39.8.3 debug mld snooping all/packet/event/timer/mfc

Command: debug mld snooping all/packet/event/timer/mfc

no debug mld snooping all/packet/event/timer/mfc

Function: Enable the debugging of the switch MLD Snooping; the “no” form of this command disables the debugging.

Command Mode: Admin Mode

Default: The MLD Snooping Debugging of the switch is disabled by default

Usage Guide: This command is used for enabling the switch MLD Snooping debugging, which displays the MLD data packet message processed by the switch——packet, event messages——event, timer messages——timer,messages of down streamed hardware entry——mfc,all debug messages——all.

39.8.4 ipv6 mld snooping

Command: ipv6 mld snooping

no ipv6 mld snooping

Function: Enable the MLD Snooping function on the switch; the “**no ipv6 mld snooping**” command disables MLD Snooping.

Command Mode: Global Mode

Default: MLD Snooping disabled on the switch by default

Usage Guide: Enable global MLD Snooping on the switch, namely allow every vlan to be configured with MLD Snooping; the “no” form of this command will disable MLD Snooping on all the vlans as well as the global MLD snooping

Example: Enable MLD Snooping under global mode.

```
Switch (config)#ipv6 mld snooping
```

39.8.5 ipv6 mld snooping vlan

Command: ipv6 mld snooping vlan <*vlan-id*>

no ipv6 mld snooping vlan <*vlan-id*>

Function: Enable MLD Snooping on specified VLAN; the “no” form of this command disables MLD Snooping on specified VLAN.

Parameter: <*vlan-id*> is the id number of the VLAN, with a valid range of <1-4094>.

Command Mode: Global Mode

Default: MLD Snooping disabled on VLAN by default

Usage Guide: To configure MLD snooping on certain VLAN, the global MLD snooping should be first enabled. Disable MLD snooping on specified VLAN with the no ipv6 mld snooping vlan vid command

Example: Enable MLD snooping on VLAN 100 under global mode.

```
Switch (config)#ipv6 mld snooping vlan 100
```

39.8.6 ipv6 mld snooping vlan immediate-leave

Command: ipv6 mld snooping vlan <*vlan-id*> immediate-leave

no ipv6 mld snooping vlan <*vlan-id*> immediate-leave

Function: Enable immediate-leave function of the MLD protocol in specified VLAN; the “no” form of this command disables the immediate-leave function of the MLD protocol

Parameter: <*vlan-id*> is the id number of specified VLAN, with valid range of <1-4094>.

Command Mode: Global Mode

Default: Disabled by default

Usage Guide: Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.

Example: Enable the MLD immediate-leave function on VLAN 100.

```
Switch (config)#ipv6 mld snooping vlan 100 immediate-leave
```

39.8.7 ipv6 mld snooping vlan l2-general-querier

Command: ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

no ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

Function: Set the VLAN to Level 2 general querier.

Parameter: *vlan-id*: is the id number of the VLAN, with a valid range of <1-4094>

Command Mode: Global Mode

Default: VLAN is not a MLD Snooping L2 general querier by default.

Usage Guide: It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this VLAN, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port.

Comment: There are three ways to learn mrouter port in MLD Snooping:

1. The port which receives MLD query messages
2. The port which receives multicast protocol packets and support PIM
3. The port statically configured.

Example: Set VLAN 100 to L2 general querier.

```
Switch (config)# ipv6 mld snooping vlan 100 l2-general-querier
```

39.8.8 ipv6 mld snooping vlan limit

Command: ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}

no ipv6 mld snooping vlan < *vlan-id* > limit

Function: Configure number of groups the MLD snooping can join and the maximum number of sources in each group.

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

g_limit: <1-65535>, max number of groups joined

s_limit: <1-65535>, max number of source entries in each group, consisting of include source and exclude source

Command Mode: Global Mode

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on VLAN. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 limit group 300
```

39.8.9 ipv6 mld snooping vlan mrouter-port interface

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>] <*ifname*>

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>] <*ifname*>

Function: Set the static mrouter port of the VLAN; the “no” form of this command cancels the configuration.

Parameter: *vlan-id*: VLAN id, the valid range is<1-4094>

***Ehternet*:** name of Ethernet port

***Ifname*:** Name of interface

***port-channel*:** port aggregate

Command Mode: Global Mode

Default: When a port is made static and dynamic mrouter port at the same time, it’s the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the “no” form of this command.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/13
```

39.8.10 ipv6 mld snooping vlan mrpt

Command: ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*>

no ipv6 mld snooping vlan <*vlan-id*> mrpt

Function: Configure the keep-alive time of the mrouter port.

Parameter: *vlan-id*: VLAN id, the valid range is <1-4094>

***value*:** mrouter port keep-alive time with a valid range of <1-65535> secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the VLAN.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 mrpt 100
```

39.8.11 ipv6 mld snooping vlan query-interval

Command: ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-interval

Function: Configure the query interval.

Parameter: *vlan-id*: VLAN id, the valid range is <1-4094>

***value*:** query interval, valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 125s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query-interval 130
```

39.8.12 ipv6 mld snooping vlan query-mrsp

Command: ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The “no” form of this command restores the default value.

Parameter: *vlan-id*: VLAN id, the valid range is<1-4094>

***value*:** the valid range is <1-25> secs .

Command Mode: Global Mode

Default: 10s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18
```

39.8.13 ipv6 mld snooping vlan query-robustness

Command: ipv6 mld snooping vlan <vlan-id> query-robustness <*value*>

no ipv6 mld snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness; the "no" form of this command restores to the default value.

Parameter: *vlan-id*: VLAN id, the valid range is <1-4094>

***value*:** the valid range is <2-10>.

Command Mode: Global Mode

Default: 2

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3
```

39.8.14 ipv6 mld snooping vlan static-group

Command: ipv6 mld snooping vlan<vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME>

no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME>

Function: Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

Parameter: *vlan-id*: ranging between <1-4094>

X:X::X:X:The address of group or source.

ethernet: Name of Ethernet port

port-channel: Port aggregation

ifname: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

```
Switch(config)#ip igmp snooping vlan 1 static-group ff1e::15 source 2000::1 interface ethernet 1/1
```

39.8.15 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time; the “no” form of this command restores the default value.

Parameter: ***vlan-id*****:** VLAN id, valid range: <1-4094>

value**:** valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270
```

39.8.16 show ipv6 mld snooping

Command: show ipv6 mld snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the number of VLAN specified to display the MLD Snooping messages

Command Mode: Admin Mode

Usage Guide: If no VLAN number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which VLAN the MLD Snooping is enabled and configured l2-general-querier. If a VLAN number is specified, the detailed MLD Snooping messages of this VLAN will be displayed.

Example:

1. Summary of the switch MLD snooping

```
Switch(config)#show ipv6 mld snooping
Global mld snooping status:   Enabled
L3 multicasting:              running
Mld snooping is turned on for vlan 1(querier)
Mld snooping is turned on for vlan 2
---------------------------------
```

Displayed Information Explanation
Global mld snooping status Whether or not the global MLD Snooping is enabled on the switch
L3 multicasting Whether or not the layer 3 multicast protocol is running on the switch.

Mld snooping is turned on for vlan 1(querier) On which VLAN of the switch is enabled MLD Snooping, if the VLAN are l2-general-querier.

2. Display the detailed MLD Snooping information of vlan1

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1

Mld snooping L2 general querier                    :Yes(COULD_QUERY)
Mld snooping query-interval                        :125(s)
Mld snooping max reponse time                       :10(s)
Mld snooping robustness                             :2
Mld snooping mrouter port keep-alive time           :255(s)
Mld snooping query-suppression time                 :255(s)

MLD Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups          Sources          Ports              Exptime    System Level
Ff1e::15        (2000::1)        Ethernet1/8        00:04:14       V2
                (2000::2)        Ethernet1/8        00:04:14       V2

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/2
```

Displayed information Explanation
Mld snooping L2 general querier whether or not l2-general-querier is enabled on vlan, the querier display status is set to could-query or suppressed
Mld snooping query-interval Query interval time of the vlan
Mld snooping max reponse time Max response time of this vlan
Mld snooping robustness

Robustness configured on the vlan
Mld snooping mrouter port keep-alive time Keep-alive time of the dynamic mrouter on this vlan
Mld snooping query-suppression time timeout of the vlan as l2-general-querier at suppressed status.
MLD Snooping Connect Group Membership Group membership of the vlan, namely the correspondence between the port and （S,G）.
Mld snooping vlan 1 mrouter port Mrouter port of the vlan, including both static and dynamic.

Chapter 40 Commands for Multicast VLAN

40.1 multicast-vlan

Command: multicast-vlan

no multicast-vlan

Function: Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Multicast VLAN function not enabled by default.

Usage Guide: The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.

Examples:

Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan

40.2 multicast-vlan association

Command: multicast-vlan association <*vlan-list*>

no multicast-vlan association <*vlan-list*>

Function: Associate several VLANs with a multicast VLAN; the “no” form of this command cancels the association relations.

Parameter: <*vlan-list*> the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.

Command Mode: VLAN Mode.

Default: The multicast VLAN is not associated with any VLAN by default.

Usage Guide: After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Examples:

Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan association 3, 4

Chapter 41 Commands for ACL

41.1 absolute-periodic/periodic

Command: [no] absolute-periodic {Monday|Tuesday|Wednesday|Thursday|Friday |Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday} <end_time>

[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|d aily| weekdays | weekend} <start_time> to <end_time>

Functions: Define the time-range of different commands within one week, and every week to circulate subject to this time.

Parameters:

Friday （Friday)

Monday （Monday)

Saturday （Saturday)

Sunday （Sunday)

Thursday （Thursday）

Tuesday （Tuesday)

Wednesday （Wednesday)

daily （Every day of the week）

weekdays （Monday thru Friday）

weekend （Saturday thru Sunday）

start_time start time ,HH:MM:SS (hour: minute: second)

end_time end time,HH:MM:SS (hour: minute: second)

Remark: time-range polling is one minute per time, so the time error shall be <= one minute.

Command Mode: time-range mode

Default: No time-range configuration.

Usage Guide: Periodic time and date. The definition of period is specific time period of Monday to Saturday and Sunday every week.

day1 hh:mm:ss To day2 hh:mm:ss or

{[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

Examples: Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.

Switch(config)#time-range admin_timer
Switch(Config-Time-Range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00 Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.
Switch(Config-Time-Range-admin_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

41.2 absolute start

Command: [no] absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]

Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.

Parameters: *start_time* : start time, HH:MM:SS (hour: minute: second)

***end_time* :** end time, HH:MM:SS (hour: minute: second)

***start_data* :** start data, the format is, YYYY.MM.DD （ year.month.day ）

***end_data* :** end data, the format is, YYYY.MM.DD（year.month.day）

Remark: time-range is one minute per time, so the time error shall be <= one minute.

Command Mode: Time-range mode

Default: No time-range configuration.

Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

Switch(config)#Time-range admin_timer
Switch(Config-Time-Range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

41.3 access-list (ip extended)

Command: access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} tcp {{ <*sIpAddr*> <*sMask*> } | any-source | {host-source <*sIpAddr*> }} [s-port { <*sPort*> | *range* <*sPortMin*> <*sPortMax*> }] {{ <*dIpAddr*> <*dMask*> } | any-destination | {host-destination <*dIpAddr*> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

access-list <num> {deny | permit} udp {{ <*sIpAddr*> <sMask> } | any-source | {host-source <*sIpAddr*> }} [s-port { <sPort> | *range* <*sPortMin*> <sPortMax>] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <*dPort*> | range <dPortMin> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

access-list <*num*> {deny | permit} {eigrp | *gre* | igrp | ipinip | ip | ospf | <protocol-num> } {{ <*sIpAddr*> <*sMask*> } | any-source | {host-source <sIpAddr> }} {{ <*dIpAddr*> <dMask> } | any-destination | *{host-destination* <dIpAddr> }} [precedence <*prec*>] [tos <*tos*>][time-range <time-range-name>]

no access-list <*num*>

Functions: Create a numeric extended IP access rule to match specific IP protocol or all IP protocol; if

access-list of this coded numeric extended does not exist, thus to create such a access-list.

Parameters: *<num>* is the No. of access-list, 100-299; ***<protocol>* is the No. of upper-layer protocol of ip, 0-255; *<sIpAddr>*** is the source IP address, the format is dotted decimal notation; ***<sMask >*** is the reverse mask of source IP, the format is dotted decimal notation; ***<dIpAddr>*** is the destination IP address, the format is dotted decimal notation; ***<dMask>*** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position1;***<igmp-type>***,the type of igmp, 0-15; ***<icmp-type>***, the type of icmp, 0-255;**<icmp-code>,** protocol No. of icmp, 0-255;**<prec>**, IP priority, 0-7; ***<tos>***, to value, 0-15; ***<sPort>,*** source port No., 0-65535; ***<sPortMin>,*** the down boundary of source port; ***<sPortMax>,*** the up boundary of source port; ***<dPortMin>,*** the down boundary of destination port; ***<dPortMax>,*** the up boundary of destination port; ***<dPort>,*** destination port No., 0-65535; ***<time-range-name>***, the name of time-range.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 200-299 can configure not continual reverse mask of IP address.

<igmp-type> represent the type of IGMP packet, and usual values please refer to the following description:

17(0x11): IGMP QUERY packet

18(0x12): IGMP V1 REPORT packet

22(0x16): IGMP V2 REPORT packet

23(0x17): IGMP V2 LEAVE packet

34(0x22): IGMP V3 REPORT packet

19(0x13): DVMR packet

20(0x14): PIM V1 packet

Particular notice: The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

Examples: Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32
```

41.4 access-list (ip standard)

Command: access-list *<num>* {deny | permit} {{*<sIpAddr>* *<sMask >*} | any-source| {host-source *<sIpAddr>*}}

no access-list *<num>*

Functions: Create a numeric standard IP access-list. If this access-list exists, then add a rule list; the "**no access-list *<num>***"operation of this command is to delete a numeric standard IP access-list.

Parameters: *<num>* is the No. of access-list, 100-199; ***<sIpAddr>*** is the source IP address, the format is dotted decimal notation; ***<sMask >*** is the reverse mask of source IP, the format is dotted decimal

notation.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.

```
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
```

```
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255
```

41.5 access-list(mac extended)

Command: access-list <*num*> {deny | permit} {any-source-mac | {host-source-mac <*host_smac*>} | {<*smac*> <*smac-mask*>}} {any-destination-mac | {host-destination-mac <*host_dmac*>} | {<*dmac*> <*dmac-mask*>}} {untagged-eth2|tagged-eth2| untagged-802-3 |tagged-802-3}[<*offset1*> <*length1*> <*value1*> [<*offset2*> <*length2*> <*value2*> [<*offset3*> <*length3*> <*value3*> [<*offset4*> <*length4*> <*value4*>]]]]]

no access-list <*num*>

Functions: Define a extended numeric MAC ACL rule, "**no access-list <*num*>**" command deletes an extended numeric MAC access-list rule.

Parameters:

<num> is the access-list No. which is a decimal's No. from 1100-1199; ***deny*** if rules are matching, deny access; ***permit*** if rules are matching, permit access; ***<any-source-mac>*** any source address; ***<any-destination-mac>*** any destination address; ***<host_smac>, <smac>*** source MAC address; ***<smac-mask>*** mask (reverse mask) of source MAC address; ***<host_dmac> , <dmac>*** destination MAC address; ***<dmac-mask>*** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet. **Offset(x)** the offset from the packet head, the range is (12-79), the windows must start from the back of source MAC, and the windows cannot superpose each other, and that is to say: Offset(x+1) must be longer than Offset(x)+len（x）; ***Length(x)*** length is 1-4 , and **Offset(x)+Length(x)** should not be longer than 80（currently should not be longer than 64）; ***Value(x)*** hex expression, **Value range:** when **Length(x)** =1, it is 0-ff , when **Length(x)** =2, it is 0-ffff , when **Length(x)** =3, it is0-ffffff, when **Length(x)** =4, it is 0-ffffffff ;

For **Offset(x),** different types of data frames are with different value ranges:

for untagged-eth2 type frame: <12～52>

for untagged-802.2 type frame: <12～60>

for untagged-eth2 type frame: <12～56>

for untagged-eth2 type frame: <12～64>

Command Mode: Global mode

Default Configuration: No access-list configured

Usage Guide: When the user assign specific <*num*> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 17th and 18th byte is 0x08 , 0x0 to pass.

```
Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 16 2
0800
```

41.6 access-list(mac-ip extended)

Command:

access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|
{host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>]
[tos <*tos*>][time-range<*time-range-name*>]
access-list<*num*>{deny|permit}{any-source-mac|
{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}
[<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]
access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*>
<*smac-mask*> }}{any-destination-mac| {host-destination-mac <*host_dmac*> }|{ <*dmac*>
<*dmac-mask*> }}tcp {{ <*source*> <*source-wildcard*> }|any-source| {host-source
<*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*>
<*destination-wildcard*> } | any-destination | {host-destination <*destination-host-ip*> }} [d-port
{ <*port3*> | *range* <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence
<*precedence*>] [tos <*tos*>] [time-range <*time-range-name*>]
access-list <num> {deny|permit}{any-source-mac| {host-source-mac <host_smac> }|{ <smac>
<smac-mask> }}{any-destination-mac| {host-destination-mac <*host_dmac*> }|{ <*dmac*>
<*dmac-mask*> }}udp {{ <*source*> <*source-wildcard*> }|any-source| {host-source
<*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*>
<destination-wildcard> }|*any-destination*| {host-destination
<destination-host-ip> }}[d-port{ <port3> | *range* <dPortMin> <*dPortMax*> }] [precedence
<*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]
access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*>
<*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*>
<*dmac-mask*> }} {eigrp|gre|igrp|ip|ipinip|ospf|{ <*protocol-num*> }} {{ <source>
<*source-wildcard*> }|any-source|{host-source <*source-host-ip*> }} {{ <*destination*>
<*destination-wildcard*> }|any-destination| {host-destination <*destination-host-ip*> }} [precedence
<precedence>] [tos <*tos*>][time-range <time-range-name>]

Functions: Define a extended numeric MAC-IP ACL rule, 'No' command deletes a extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3299;**deny** if rules are

matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac , smac**: source MAC address; **smac-mask: mask** (reverse mask) of source MAC address ; **host_dmac , dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip, source** No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host:** means the address is the that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional):** means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; **d-port(optional):** means need to match TCP/UDP destination interface; ***<sPortMin>,*** the down boundary of source port; ***<sPortMax>,*** the up boundary of source port; **port3(optional):** value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>,*** the down boundary of destination port;<dPortMax>, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**,(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence** (optional) packets can be filtered by priority which is a number from 0-7; **tos** (optional) packets can be filtered by service type which ia number from 0-15; **icmp-type** (optional) ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code** (optional) ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type** (optional) ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; **<time-range-name>**, name of time range

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address.

Examples: Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100 and destination interface 40000.

```
Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF
any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000
```

41.7 access-list(mac standard)

Command: access-list <*num*> {deny|permit} {any-source-mac | {host-source-mac <*host_smac*> } | {<*smac*> <*smac-mask*>} }

no access-list <num>

Functions: Define a standard numeric MAC ACL rule, '**no access-list <num>**' command deletes a standard numeric MAC ACL access-list rule.

Parameters: ***<num>*** is the access-list No. which is a decimal's No. from 700-799; ***deny*** if rules are matching, deny access; ***permit*** if rules are matching, permit access; ***<host_smac>***, ***<sumac>*** source MAC address; ***<sumac-mask>*** mask (reverse mask) of source MAC address.

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab.

```
Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00
```

```
Switch(config)# access-list 700 deny    00-00-00-00-00-ab 00-00-00-FF-00-00
```

41.8 clear access-group statistic interface

Command: clear access-group statistic interface { <interface-name> | ethernet <*interface-name*> }

Functions: Empty packet statistics information of assigned interfaces.

Parameters: <*interface-name*>: Interface name.

Command Mode: Admin mode

Default: None

Examples: Empty packet statistics information of interface1/1.

```
Switch#clear access-group out statistic interface ethernet 1/1
```

41.9 firewall

Command: firewall {enable | disable}

Functions: Enable or disable firewall.

Parameters: enable means to enable of firewall; **disable** means to disable firewall.

Default: It is no use if default is firewall.

Command Mode: Global mode

Usage Guide: Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.

Examples: Enable firewall.

```
Switch(config)#firewall enable
```

41.10 firewall default

Command: firewall default {permit | deny [ipv4 | ipv6 | all]}

Functions: Configure default actions of firewall.

Parameters: permit means to permit data packets to pass; **deny** [ipv4 | ipv6 | all] means to deny ipv4|ipv6 all data packets to pass. If configure the default deny *, cancel it by default permit.

Command Mode: Global Mode.

Default: Default action is permit.

Usage Guide: This command only influences all packets from the port entrance.

Examples: Configure firewall default action as permitting packets to pass.

```
Switch(config)#firewall default permit
```

41.11 ip access extended

Command: ip access extended <*name*>

no ip access extended <*name*>

Function: Create a named extended IP access list. The no prefix will remove the named extended IP access list including all the rules.

Parameters: <name> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a extended IP access list name tcpFlow.

```
Switch(config)#ip access-list extended tcpFlow
```

41.12 ip access standard

Command: ip access standard <*name*>

no ip access standard <*name*>

Function: Create a named standard access list. The no prefix will remove the named standard access list including all the rules in the list.

Parameters: <*name*> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a standard IP access list name ipFlow.

```
Switch(config)#ip access-list standard ipFlow
```

41.13 ipv6 access-list

Command: ipv6 access-list <*num-std*> {deny | permit} {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}}

ipv6 access-list <num-ext> {deny | permit} icmp {{ <sIPv6Prefix/sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl> *][time-range* <time-range-name>]

ipv6 access-list <*num-ext*> {deny | permit} tcp {{ <*sIPv6Prefix/<sPrefixlen*> } | any-source | {host-source <*sIPv6Addr*> }} [s-port { <sPort> | range <sPortMin> <*sPortMax*> }] {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination <dIPv6Addr> }} [dPort { <dPort> | range <dPortMin> <dPortMax> }] [syn | *ack* | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*flowlabel*>][time-range <*time-range-name*>]

ipv6 access-list <num-ext> {deny | permit} udp {{ <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source <*sIPv6Addr*> }} [s-port { <sPort> | *range* <sPortMin> <sPortMax> }] {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination <dIPv6Addr> }} [dPort { <*dPort*> | range <dPortMin> <*dPortMax*> }] [dscp <*dscp*>] [flow-label <*flowlabel*>][time-range <*time-range-name*>]

ipv6 access-list <*num-ext*> {deny | permit} <next-header> { <*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <sIPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [dscp <dscp>] [flow-label <fl>][time-range <*time-range-name*>]

no ipv6 *access-list* { <num-std> | <num-ext> }

Functions: Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list {<*num-std*>|<*num-ext*>}** "command deletes a numbered standard IP access-list.

Parameters: <*num-std*> is the list number ,list range is between 500～599; <num-ext> is the list number ,list range is between 600～699; **<*sIPv6Prefix*>** is the prefix of the ipv6 source address; **<sPrefixlen >** is the length of prefix of the ipv6 source address, range is between 1～128; **<sIPv6Addr>** is the ipv6 source address; **<dIPv6Prefix>** is the prefix of the ipv6 destination address; **<dPrefixlen** > is the length of prefix of the ipv6 destination address, range is between 1～128; **<dIPv6Addr>** is the ipv6 destination address; **<icmp-type>**, the type of icmp; **<icmp-code>**，the protocol code of icmp; <dscp>，IPv6 priority, range from 0 to 63; **<flowlabel>**，value of flow tag, range from 0 to 1048575; **syn，ack，urg，rst，fin，psh，tcp** label position; **<sPort>**, source port No., 0-65535; **<sPortMin>**, the down boundary of source port; **<sPortMax>**, the up boundary of source port; **<dPort>**，destination port No., range from 0 to 65535; ***<dPortMin>,*** the down boundary of destination port; ***<dPortMax>,*** the up boundary of destination port; ***<next-header>***，the next header of IPv6, range from 0 to 255; ***<time-range-name>,*** the name of time-range.

Command Mode: Global Mode.

Default: No access-list configured.

Usage Guide: Creates a numbered 520 standard IP access-list first time, the following configuration will add to the current access-list.

Examples: Creates a numbered 520 standard IP access-list, allow the source packet from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address

2003:1:2::1/48 pass through.

Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48

```
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48
```

41.14 ipv6 access standard

Command: ipv6 access-list standard <*name*>

no ipv6 access-list standard <*name*>

Function: Create a name-based standard IPv6 access list; the "**no ipv6 access-list standard<*name*>**"command deletes the name-based standard IPv6 access list (including all entries).

Parameter: <*name*> is the name for access list, the character string length is from 1-32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create a standard IPv6 access list named "ip6Flow".

Switch(config)#ipv6 access-list standard ip6Flow

```
Switch(config)#ipv6 access-list standard ip6Flow
```

41.15 ipv6 access extended

Command: ipv6 access-list extended <*name*>

no ipv6 access-list extended <*name*>

Function: Create a name-based extended IPv6 access list; the "**no ipv6 access-list extended<*name*>**" command delete the name-based extended IPv6 access list.

Parameter: <*name*> is the name for access list, the character string length is from 1 to 32.

Command Mode: Global Mode.

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create an extensive IPv6 access list named "tcpFlow".

```
Switch (config)#ipv6 access-list extended tcpFlow
```

41.16 {ip|ipv6|mac|mac-ip} access-group

Command: {ip|ipv6|mac|mac-ip} access-group <*name*> {in} [traffic-statistic]

no {ip|mac} access-group <*name*> {in}

Function: Apply an access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options; the no command deletes access-list binding on the port.

Parameter: <*name*> is the name for access list, the character string length is from 1-32.

Command Mode: Physical Port Mode

Default: The entry of port is not bound ACL.

Usage Guide: One port can bind ingress rules.

There are four kinds of packet head field based on concerned: MAC ACL, IP ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data packet matches multi types of eight ACLs. The strict priorities are specified for each ACL based on outcome veracity. It can determine final behavior of packet filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1 · Each port can bind a MAC-IP ACL, a IP ACL, a IPv6 ACL and a MAC ACL;

2 · When binding 2 ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below,

Ingress IPv6 ACL

Ingress MAC-IP ACL

Ingress MAC ACL;

Ingress IP ACL;

Example: Binding AAA access-list to entry direction of port.

```
Switch(Config-If-Ethernet1/5)#ip access-group aaa in
```

41.17 mac access extended

Command: mac-access-list extended <*name*>

no mac-access-list extended <name>

Functions: Define a name-manner MAC ACL or enter access-list configuration mode, "**no mac-access-list extended <*name*>**" command deletes this ACL.

Parameters: <*name*> name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default Configuration: No access-lists configured.

Usage Guide: After assigning this commands for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC ACL named mac_acl.

Switch(Config-Mac-Ext-Nacl-mac_acl)#

```
Switch(config)# mac-access-list extended mac_acl
```

```
Switch(Config-Mac-Ext-Nacl-mac_acl)#
```

41.18 mac-ip access extended

Command: mac-ip-access-list extended <*name*>

no mac-ip-access-list extended <*name*>

Functions: Define a name-manner MAC-IP ACL or enter access-list configuration mode, "**no mac-ip-access-list extended <*name*>**" command deletes this ACL.

Parameters: <*name*>: name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).

Command Mode: Global Mode.

Default: No named MAC-IP access-list.

Usage Guide: After assigning this commands for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC-IP ACL named macip_acl.

```
Switch(config)# mac-ip-access-list extended macip_acl
```

```
Switch(Config-MacIp-Ext-Nacl-macip_acl)#
```

41.19 permit | deny (ip extended)

Command: [no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} tcp {{ <*sIpAddr*> <*sMask*> } | any-source | {host-source <*sIpAddr*> }} [s-port { <*sPort*> | *range* <*sPortMin*> <*sPortMax*> }] {{ <*dIpAddr*> <*dMask*> } | any-destination | {host-destination <*dIpAddr*> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

[no] {deny | permit} *udp* {{ <sIpAddr> <*sMask*> } | any-source | {host-source <*sIpAddr*> }} [s-port { <sPort> | range <*sPortMin*> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <*dPort*> | range <dPortMin> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | < *protocol-num* >} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Create a name extended IP access rule to match specific IP protocol or all IP protocol.

Parameters: <*sIpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dIpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position 1; **<*igmp-type*>**, the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255 ; **<icmp-code>,** protocol No. of icmp, 0-255; **<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>,** source port No., 0-65535; **<*sPortMin*>,** the down boundary of *source port;* <sPortMax>, the up boundary of source port; **<*dPort*>,** destination port No. 0-65535; **<*dPortMin*>,** the down boundary of destination port; **<*dPortMax*>,** the up boundary of destination port; **<*time-range-name*>,** time range name.

Command Mode: Name extended IP access-list configuration mode

Default: No access-list configured.

Examples: Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)# access-list ip extended udpFlow
```

Switch(Config-IP-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IP-Ext-Nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port 32

41.20 permit | deny(ip standard)

Command: {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

Functions: Create a name standard IP access rule, and "**no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}**" action of this command deletes this name standard IP access rule.

Parameters: <*sIpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation.

Command Mode: Name standard IP access-list configuration mode

Default: No access-list configured.

Example: Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

Switch(config)# access-list ip standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

41.21 permit | deny(ipv6 extended)

Command:[no]{deny|permit}icmp{{<*sIPv6Prefix*/*sPrefixlen*>|any|{host<*sIPv6Addr*>}}{<*dIPv6Prefix/dPrefixlen*>|any-destination|{host-destination<*dIPv6Addr*>}}[<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>] [time-range <*time-range-name*>]

[no] {deny | permit} tcp { <*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*> }} [s-port { <sPort> | *range* <*sPortMin*> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <*dPortMin*> <*dPortMax*> }] [syn | *ack* | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | permit} udp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <*sIPv6Addr*> }} [s-port { <sPort> | *range* <sPortMin> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <*dPort*> | *range* <dPortMin> <*dPortMax*> }] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | permit} <*next-header*> {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | permit} {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label <*fl*>] [time-range<*time-range-name*>]

Function: Create an extended nomenclature IPv6 access control rule for specific IPv6 protocol.

Parameter:<*sIPv6Addr*> is the source IPv6 address;**<*sPrefixlen*>** is the length of the IPv6 address prefix, the range is 1～128;**<*dIPv6Addr*>** is the destination IPv6 address;**<*dPrefixlen*>** is the length of the IPv6 address prefix, the range is 1～128;**<*igmp-type*>**,type of the IGMP;**<*icmp-type*>**,icmp type;**<*icmp-code*>**,icmp protocol number;**<*dscp*>**,IPv6 priority ,the range is 0～63; **<*flowlabel*>**,value of the flow label, the range is 0～1048575;**syn**,**ack**,**urg**,**rst**,**fin**,**psh**,**tcp** label position; **<*sPort*>,** source port number, the range is 0～65535; **<*sPortMin*>,** the down boundary of source port; <sPortMax>, the up boundary of source port; <dPort>, destination port number, the range is 0～65535; **<*dPortMin*>,** the down boundary of destination port; **<*dPortMax*>,** the up boundary of destination port. **<*next-header*>,** the IPv6 next-header. **<*time-range-name*>,** time range name.

Command Mode: IPv6 nomenclature extended access control list mode

Default: No access control list configured.

Example: Create an extended access control list named udpFlow, denying the igmp packets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

Switch(config)#ipv6 access-list extended udpFlow
Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1 dPort 32

41.22 permit | deny(ipv6 standard)

Command: [no] {deny | permit} {{<*sIPv6Prefix*/*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}}

Function: Create a standard nomenclature IPv6 access control rule; the “no” form of this command deletes the nomenclature standard IPv6 access control rule.

Parameter: <*sIPv6Prefix*> is the prefix of the source IPv6 address,**<*sPrefixlen*>** is the length of the IPv6 address prefix, the valid range is 1~128. **<*sIPv6Addr*>** is the source IPv6 address.

Command Mode: Standard IPv6 nomenclature access list mode

Default: No access list configured by default.

Usage Guide:

Example: Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.

Switch(config)#ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48

41.23 permit | deny(mac extended)

Command:

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*>

<*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [cos <*cos-val*> [<*cos-bitmask*>][vlanid <vid-value> [<vid-mask>][*ethertype* <protocol> [<*protocol-mask*>]]]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [ethertype <protocol> [<protocol-mask>]]

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [vlanid <vid-value> [<vid-mask>][ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit} *{any-source-mac|{host-source-mac* <host_smac> *}|{* <*smac*> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <*dmac*> <dmac-mask> }} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <*dmac-mask*> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <smac-mask> }} *{any-destination-mac|{host-destination-mac* <host_dmac> }|{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]

Functions: Define an extended name MAC ACL rule, and 'no' command deletes this extended name IP access rule.

Parameters: any-source-mac: any source of MAC address; **any-destination-mac**: any destination of MAC address; **host_smac**, **smac**: source MAC address; **smac-mask**: mask (reverse mask) of source MAC address ; **host_dmac**, **dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet; ***cos-val*****:** cos value, 0-7; ***cos-bitmask*****:** cos mask, 0-7reverse mask and mask bit is consecutive; ***vid-value*****:** VLAN No, 1-4094; ***vid-bitmask*****:** VLAN mask, 0-4095, reverse mask and mask bit is consecutive; ***protocol*****:** specific Ethernet protocol No., 1536-65535; ***protocol-bitmask*****:** protocol mask, 0-65535, reverse mask and mask bit is consecutive.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

Command Mode: Name extended MAC access-list configuration mode

Default configuration: No access-list configured.

Example: The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data packet.

Switch(config)# mac-access-list extended macExt
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3
Switch(Config-Mac-Ext-Nacl-macExt)# deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802

41.24 permit | deny(mac-ip extended)

Command:

[no] {deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} icmp{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} igmp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }| { <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}tcp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port { <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <*destination-wildcard*> } | any-destination| {host-destination <*destination-host-ip*> }} [d-port { <*port3*> | range <*dPortMin*> <*dPortMax*> }] [ack＋fin＋psh＋rst＋urg＋syn] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <*smac*> <smac-mask> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }| { <dmac> <*dmac-mask*> }}udp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <destination-wildcard> }|any-destination| *{host-destination* <destination-host-ip> }} [d-port { <port3> | range <*dPortMin*> <dPortMax> }] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*> <*smac-mask*>*}*}{any-destination-mac|{host-destination-mac<*host_dmac*>}| {<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Define an extended name MAC-IP ACL rule, 'No' form deletes one extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3199; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac**, smac: source MAC address; smac-mask: mask (reverse mask) of source MAC address ; **host_dmac** , dmas destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip**, source No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional)**: means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; ***<sPortMin>,*** the down boundary of source port; ***<sPortMax>,*** the up boundary of source port; d-port(optional): means need to match TCP/UDP destination interface; **port3(optional):** value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>,*** the down boundary of destination port; ***<dPortMax>,*** the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**, (optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence (optional)** packets can be filtered by priority which is a number from 0-7; **tos (optional)** packets can be filtered by service type which ia number from 0-15; **icmp-type (optional)** ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code (optional)** ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type (optional)** ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255;

<time-range-name>, name of time range.

Command Mode: Name extended MAC-IP access-list configuration mode

Default: No access-list configured.

Examples: Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination port 40000.

```
Switch(config)# mac-ip-access-list extended macIpExt
```

```
Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000
```

41.25 show access-lists

Command: show access-lists [<*num*>|<*acl-name*>]

Functions: Reveal ACL of configuration.

Parameters: <*acl-name*>, specific ACL name character string; ***<num>,*** specific ACL No.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When not assigning names of ACL, all ACL will be revealed, used x time（s）indicates the times of ACL to be used.

Examples:

```
Switch#show access-lists
access-list 10(used 0 time(s))
    access-list 10 deny any-source

access-list 100(used 1 time(s))
    access-list 100 deny ip any any-destination
    access-list 100 deny tcp any any-destination

access-list 1100(used 0 time(s))
    access-list 1100 permit any-source-mac any-destination-mac tagged-eth2   14 2 0800
 access-list 3100(used 0 time(s))
    access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000
```

Displayed information Explanation
access-list 10(used 1 time(s)) Number ACL10, 0 time to be used
access-list 10 deny any

Deny any IP packets to pass
access-list 100(used 1 time(s)) Nnumber ACL10, 1 time to be used
access-list 100 deny ip any any-destination Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any any-destination Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800 Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass.
access-list 3100 permit any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000 Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination interface 40000

41.26 show access-group

Command: show access-group [interface {ethernet IFNAME| vlan <*1-4094*>]

Functions: Reveal tying situation of ACL on port.

Parameters: IFNAME*,* Interface name. ***<1-4094 >*** Vlan ID.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When not assigning interface names, all ACL tied to port will be revealed.

Examples:

```
Switch#show access-group
interface name: Ethernet 1/1
    IP Ingress access-list used is 100, traffic-statistics Disable.
Interface VLAN 100:
Ethernet1/4:    IP Ingress access-list used is 100, packet(s) number is 0.
Ethernet1/5:    IP Ingress access-list used is 100, packet(s) number is 0.
Ethernet1/6:    IP Ingress access-list used is 100, packet(s) number is 0.
```

Displayed information Explanation
interface name: Ethernet 1/1

Tying situation on port Ethernet1/1
the ingress acl use in firewall is 111. No. 111 numeric expansion ACL tied to entrance of port Ethernet1/2
interface VLAN 100 Tying situation on VLAN 100
packet(s) number is 10 Number of packets matching this ACL rule

41.27 show firewall

Command: show firewall

Functions: Reveal configuration information of packet filtering functions.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Examples:

```
Switch#show firewall
Firewall status: Enable.
Firewall default rule: Permit
```

Displayed information Explanation
fire wall is enable Packet filtering function enabled
the default action of firewall is permit Default packet filtering function is permit

41.28 show ipv6 access-lists

Command: show ipv6 access-lists [<*num*>|<*acl-name*>]

Function: Show the configured IPv6 access control list.

Parameter:<num> is the number of specific access control list, the valid range is 500～699,amongst 500 ～ 599 is digit standard IPv6 ACL number,600 ～ 699 is the digit extended IPv6 ACL number;<acl-name> is the nomenclature character string of a specific access control list, lengthening within 1～16.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted.

Example:

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
    ipv6 access-list 500 deny any-source

ipv6 access-list 510(used 1 time(s))
    ipv6 access-list 510 deny ip any any-destination
    ipv6 access-list 510 deny tcp any any-destination

ipv6 access-list 520(used 1 time(s))
    ipv6 access-list 520 permit ip any any-destination
```

41.29 show time-range

Command: show time-range *<word>*

Functions: Reveal configuration information of time range functions.

Parameters: *word* assign name of time-range needed to be revealed.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When not assigning time-range names, all time-range will be revealed.

Examples:

```
Switch#show time-range
time-range timer1 (inactive, used 0 times)
        absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
        absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

41.30 time-range

Command: [no] time-range *<time_range_name>*

Functions: Create the name of time-range as time range name, enter the time-range mode at the same time.

Parameters: *time_range_name*, time range name must start with letter, and the length cannot exceed 16 characters long.

Command Mode: Global mode

Default: No time-range configuration.

Usage Guide: None

Examples: Create a time-range named admin_timer.

```
Switch(config)#Time-range admin_timer
```

Chapter 42 Commands for 802.1x

42.1 debug dot1x detail

Command: debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased } interface [ethernet] <*interface-name*>

no debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased | webbased } interface [ethernet] <*interface-name*>

Function: Enable the debug information of dot1x details; the no operation of this command will disable that debug information.

Parameters: pkt-send: Enable the debug information of dot1x about sending packets;

pkt-receive: Enable the debug information of dot1x about receiving packets;

internal: Enable the debug information of dot1x about internal details;

all: Enable the debug information of dot1x about all details mentioned above;

userbased: user-based authentication;

webbased: Web-based authentication;

<*interface-name*>: the name of the interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x details, users can check the detailed processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable all debug information of dot1x details on interface1/1.

```
Switch#debug dot1x detail all interface ethernet1/1
```

42.2 debug dot1x error

Command: debug dot1x error

no debug dot1x error

Function: Enable the debug information of dot1x about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x about errors, users can check the information of errors that occur in the processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about errors.

```
Switch#debug dot1x error
```

42.3 debug dot1x fsm

Command: debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>

no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>

Function: Enable the debug information of dot1x state machine; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: all: Enable the debug information of dot1x state machine;

aksm: Enable the debug information of Authenticator Key Transmit state machine;

asm: Enable the debug information of Authenticator state machine;

basm: Enable the debug information of Backend Authentication state machine;

ratsm: Enable the debug information of Re-Authentication Timer state machine;

***<interface-name>*:** the name of the interface.

Usage Guide: By enabling the debug information of dot1x, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x state machine.

```
Switch#debug dot1x fsm asm interface ethernet1/1
```

42.4 debug dot1x packet

Command: debug dot1x packet {all | receive | send} interface *<interface-name>*

no debug dot1x packet {all | receive | send} interface *<interface-name>*

Function: Enable the debug information of dot1x about messages; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: send: Enable the debug information of dot1x about sending packets;

receive: Enable the debug information of dot1x about receiving packets;

all: Enable the debug information of dot1x about both sending and receiving packets;

***<interface-name>*:** the name of the interface.

Usage Guide: By enabling the debug information of dot1x about messages, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about messages.

```
Switch#debug dot1x packet all interface ethernet1/1
```

42.5 dot1x accept-mac

Command: dot1x accept-mac *<mac-address>* [interface *<interface-name>*]

no dot1x accept-mac *<mac-address>* [interface *<interface-name>*]

Function: Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The “no dot1x accept-mac <mac-address> [interface <interface-name>]” command deletes the entry from dot1x address filter table.

Parameters: *<mac-address>* stands for MAC address;

<interface-name> for interface name and port number.

Command mode: Global Mode.

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the

authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/5.

```
Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5
```

42.6 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Enables the EAP relay authentication function in the switch; the “no dot1x eapor enable” command sets EAP local end authentication.

Command mode: Global Mode.

Default: EAP relay authentication is used by default.

Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.

Example: Setting EAP local end authentication for the switch.

```
Switch(config)#no dot1x eapor enable
```

42.7 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enables the 802.1x function in the switch and ports: the "**no dot1x enable**" command disables the 802.1x function.

Command mode: Global Mode and Port Mode.

Default: 802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.

Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.

Example: Enabling the 802.1x function of the switch and enable 802.1x for port1/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
```

42.8 dot1x ipv6 passthrough

Command: dot1x ipv6 passthrough

no dot1x ipv6 passthrough

Function: Enable IPv6 passthrough function on a switch port, only applicable when access control mode is userbased; the no operation of this command will disable the function.

Command Mode: Port Configuration Mode.

Default Settings: IPv6 passthrough function is disabled on the switch by default.

Usage Guide: The function can only be enabled when 802.1x function is enabled both globally and on the port, with userbased being the control access mode. After it is enabled, users can send IPv6 messages without authentication.

Examples: Enable IPv6 passthrough function on port Ethernet1/12.

Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
Switch(Config-If-Ethernet1/12)#dot1x ipv6 passthrough

42.9 dot1x guest-vlan

Command: dot1x guest-vlan <*vlanid*>

no dot1x guest-vlan

Function: Set the guest-vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest-vlan.

Parameters: <*vlanid*> the specified VLAN id, ranging from 1 to 4094.

Command Mode: Port Mode.

Default Settings: There is no 802.1x guest-vlan function on the port.

User Guide: The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

- ☞ The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN.
- ☞ The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

Attention:

- ☞ There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.
- ☞ Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

Examples：Set Guest-VLAN of port Ethernet1/3 as VLAN 10.

```
Switch(Config-If-Ethernet1/3)#dot1xguest-vlan 10
```

42.10 dot1x macfilter enable

Command: dot1x macfilter enable

no dot1x macfilter enable

Function: Enables the dot1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the dot1x address filter function.

Command mode: Global Mode

Default: dot1x address filter is disabled by default.

Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.

Example: Enabling dot1x address filter function for the switch.

```
Switch(config)#dot1x macfilter enable
```

42.11 dot1x max-req

Command: dot1x max-req <*count*>

no dot1x max-req

Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the “no dot1x max-req” command restores the default setting.

Parameters: <*count*> is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.

Command mode: Global Mode.

Default: The default maximum for retransmission is 2.

Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.

Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.

```
Switch(config)#dot1x max-req 5
```

42.12 dot1x user free-resource

Command: dot1x user free-resource <*prefix*> <*mask*>

no dot1x user free-resource

Function: To configure 802.1x free resource; the no form command closes this function.

Parameter: <*prefix*> is the segment for limited resource，in dotted decimal format;

<*mask*> is the mask for limited resource，in dotted decimal format.

Command Mode: Global Mode.

Default: There is no free resource by default.

Usage Guide: This command is available only if user based access control is applied. If user based access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access control, users could access no network resources before authentication.

If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches.

To be noticed, only one free resource can be configured for the overall network.

Example: To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0.

```
Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0
```

42.13 dot1x max-user macbased

Command: dot1x max-user macbased <*number*>

no dot1x max-user macbased

Function: Sets the maximum users allowed connect to the port; the “no dot1x max-user” command restores the default setting.

Parameters: <*number*> is the maximum users allowed, the valid range is 1 to 256.

Command mode: Port configuration Mode.

Default: The default maximum user allowed is 1.

Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.

Example: Setting port 1/3 to allow 5 users.

```
Switch(Config-If-Ethernet1/3)#dot1x max-user macbased 5
```

42.14 dot1x max-user userbased

Command: dot1x max-user userbased <*number*>

no dot1x max-user userbased

Function: Set the upper limit of the number of users allowed access the specified port when using user-based access control mode; the “no dot1x max-user userbased” command is used to reset the default value.

Parameters: <*number*> the maximum number of users allowed to access the network, ranging from 1 to 1~256.

Command Mode: Port Mode.

Default Settings: The maximum number of users allowed to access each port is 10 by default.

User Guide: This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network.

Examples: Setting port 1/3 to allow 5 users.

```
Switch(Config-If-Ethernet1/3)#dot1x max-user userbased 5
```

42.15 dot1x port-control

Command: dot1x port-control {auto|force-authorized|force-unauthorized }

no dot1x port-control

Function: Sets the 802.1x authentication status; the "no dot1x port-control" command restores the default setting.

Parameters: auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.

Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **auto** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to auto.

Example: Setting port1/1 to require 802.1x authentication mode.

Switch(Config-If-Ethernet1/1)#dot1x port-control auto

```
Switch(config)#interface ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#dot1x port-control auto
```

42.16 dot1x port-method

Command: dot1x port-method {macbased | portbased | webbased | userbased advanced}

no dot1x port-method

Function: To configure the access control method of appointed interface. The no form command restores the default access control method.

Parameter: macbased means the access control method based on MAC address; **portbased** means the access control method based on port; **webbased** means the access control method based on web authentication; **userbased** means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method.

Command mode: Port Configuration Mode.

Default: Advanced access control method based on user is used by default.

Usage Guide: This command is used to configure the dot1x authentication method for the specified port. When port based authentication is applied, only one host can authenticate itself through one port. And after authentication, the host will be able to access all the resources. When MAC based authentication is applied, multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied, un-authenticated host cannot access any resources in the network.

When user based access control is applied, un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control. The standard user based access control does not limit the

access to the limited resources when the host is not authenticated yet. While the user based advanced access control can control the access to the limited resources before authentication is done.

Webbased access management is used mostly in layer switch. The global configuration of WEB authentication agent and HTTP redirection address is needed before setting the port to Webbased access management. Webbased access management is conflicted with the command of ip dhcp snooping binding user-control.

Notes: The 802.1x free resource must be configured first for standard control method based on user.

Example: To configure the standard control method based on port for Etherent1/4.

```
Switch(Config-If-Ethernet1/4)#dot1x port-method portbased
```

42.17 dot1x privateclient enable

Command: dot1x privateclient enable

no dot1x privateclient enable

Function: To configure the switch to force the authentication client to use private 802.1x authentication protocol. The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.

Command: Global Mode.

Default: Private 802.1x authentication packet format is disabled by default.

Usage Guide: To implement integrated solution, the switch must be enabled to use private 802.1x protocol, or many applications will not be able to function. If the switch forces the authentication client to use private 802.1x protocol, the standard client will not be able to work.

Example: To force the authentication client to use private 802.1x authentication protocol.

```
Switch(config)#dot1x privateclient enable
```

42.18 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]

Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

Parameters: <*interface-name*> stands for port number, omitting the parameter for all ports.

Command mode: Global Mode.

Usage Guide: This command is an Global Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.

Example: Enabling real-time re-authentication on port1/8.

```
Switch(config)#dot1x re-authenticate interface ethernet 1/8
```

42.19 dot1x re-authentication

Command: dot1x re-authentication

no dot1x re-authentication

Function: Enables periodical supplicant authentication; the “no dot1x re-authentication” command disables this function.

Command mode: Global Mode.

Default: Periodical re-authentication is disabled by default.

Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.

Example: Enabling the periodical re-authentication for authenticated users.

```
Switch(config)#dot1x re-authentication
```

42.20 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>

no dot1x timeout quiet-period

Function: Sets time to keep silent on supplicant authentication failure; the “**no dot1x timeout quiet-period**” command restores the default value.

Parameters: <*seconds*> is the silent time for the port in seconds, the valid range is 1 to 65535.

Command mode: Global Mode.

Default: The default value is 10 seconds.

Usage Guide: Default value is recommended.

Example: Setting the silent time to 120 seconds.

```
Switch(config)#dot1x timeout quiet-period 120
```

42.21 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>

no dot1x timeout re-authperiod

Function: Sets the supplicant re-authentication interval; the “**no dot1x timeout re-authperiod**” command restores the default setting.

Parameters: <*seconds*> is the interval for re-authentication, in seconds, the valid range is 1 to 65535.

Command mode: Global Mode.

Default: The default value is 3600 seconds.

Usage Guide: dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.

Example: Setting the re-authentication time to 1200 seconds.

```
Switch(config)#dot1x timeout re-authperiod 1200
```

42.22 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>

no dot1x timeout tx-period

Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.

Parameters: <*seconds*> is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.

Command mode: Global Mode.

Default: The default value is 30 seconds.

Usage Guide: Default value is recommended.

Example: Setting the EAP request frame re-transmission interval to 1200 seconds.

```
Switch(config)#dot1x timeout tx-period 1200
```

42.23 dot1x unicast enable

Command: dot1x unicast enable

no dot1x unicast enable

Function: Enable the 802.1x unicast passthrough function of switch; the no operation of this command will disable this function.

Command mode: Global Configuration Mode.

Default: The 802.1x unicast passthrough function is not enabled in global mode.

Usage Guide: The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured.

Example: Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/1.

```
Switch(config)#dot1x enable
Switch(config)# dot1x unicast enable
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#dot1x enable
```

42.24 dot1x web authentication enable

Command: dot1x web authentication enable

no dot1x web authentication enable

Function: Enable Web authentication agent, the no command disable Web authentication agent.

Parameters: None.

Default: Web authentication agent is disabled.

Command mode: Global Mode.

Usage Guide: Dot1x function must be enabled before enabling Web authentication agent. When dot1x web authentication agent is enabled, the **dot1x privateclient enable** command should not be configured.

Example: Enable the Web authentication agent function.

```
Switch(config)#dot1x web authentication enable
```

42.25 dot1x web redirect

Command: dot1x web redirect <URL>

no dot1x web redirect

Function: Set the HTTP server address for Web redirection, the no command clears the address.

Parameters: *<URL>* is HTTP server address, in dotted decimal notation.

Default: The redirection function is disabled.

Command mode: Global Mode.

Usage Guide: The Web authentication function must be enabled before setting the Web server address. The URL format is http://A.B.C.D[:E]/F, A.B.C.D is the IP address; E is the HTTP service port number, default value is 80; F is a string of character and the command do not do the validation checking on it.

Example: Set the Web redirection address as http://192.168.20.20/WebSupplicant.

```
Switch(config)#dot1x web redirect http://192.168.20.20/WebSupplicant/
```

42.26 dot1x web redirect enable

Command: dot1x web redirect enable

no dot1x web redirect enable

Function: To enable unauthenticated user to visit Web redirect function. After enable this function, if unauthenticated user try to visit Website resource not for free (The http visiting required destination port is 80 here), the switch can configure Web visiting redirect to specified website, then remind user to authenticate. The Website IP can configure in inter security management background system TrustView, only can configure IP address and not support domain name.

Parameter: None.

Command Mode: Global Mode.

Default: The unauthenticated user Web redirect function is disabled by default. Manager can configure redirect function in inter security management background system, this address can transmit to switch through private communication protocol between switch and background system.

Usage Guide:

Example: Enable the unauthenticated user to visit the redirect function through Web.

```
Switch(Config)# dot1x web redirect enable
```

42.27 show dot1x

Command: show dot1x [interface *<interface-list>*]

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: *<interface-list>* is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin and Configuration Mode.

Usage Guide: The dot1x related parameter and dot1x information can be displayed with “show dot1x” command.

Example:

1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled          no
   reauth-period           3600
   quiet-period            10
   tx-period               30
   max-req                  2
   authenticator mode      passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable
dot1x-web authentication Enable

802.1x is enabled on ethernet Ethernet1/1
Authentication Method:Port based
Max User Number:1
   Status                  Authorized
   Port-control            Auto
   Supplicant              00-30-4f-FE-2E-D3

Authenticator State Machine
   State                   Authenticated
Backend State Machine
   State                   Idle
Reauthentication State Machine
   State                   Stop

802.1X is enabled on ethernet Ethernet1/16
Authentication Method: web based
   Status                  Authorized
   Port-control            Auto
   Supplicant IP           192.168.1.11
VLAN id 2
```

Displayed information Explanation
Global 802.1x Parameters

Global 802.1x parameter information
reauth-enabled Whether re-authentication is enabled or not
reauth-period Re-authentication interval
quiet-period Silent interval
tx-period EAP retransmission interval
max-req EAP packet retransmission interval
authenticator mode Switch authentication mode
Mac Filter Enables dot1x address filter or not
MacAccessList Dot1x address filter table
Dot1x-EAPoR Authentication method used by the switch (EAP relay, EAP local end)
802.1x is enabled on ethernet Ethernet1/1 Indicates whether dot1x is enabled for the port
Authentication Method: Port authentication method (MAC-based, port-based)
Status Port authentication status
Port-control Port authorization status
Supplicant Authenticator MAC address

Authenticator State Machine Authenticator state machine status
Backend State Machine Backend state machine status
Reauthentication State Machine Re-authentication state machine status

Chapter 43 Commands for the Number Limitation Function of Port, MAC in VLAN and IP

43.1 switchport mac-address dynamic maximum

Command: switchport mac-address dynamic maximum <*value*>

no switchport mac-address dynamic maximum

Function: Set the max number of dynamic MAC address allowed by the port, and, at the same time, enable the number limitation function of dynamic MAC address on the port; "**no switchport mac-address dynamic maximum**" command is used to disable the number limitation function of dynamic MAC address on the port.

Parameters: <*value*> upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.

Examples:

Enable the number limitation function of dynamic MAC address in port 1/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport mac-address dynamic maximum 20 Disable the number limitation function of dynamic MAC address in port 1/2 mode
Switch(Config-If-Ethernet1/2)#no switchport mac-address dynamic maximum

43.2 vlan mac-address dynamic maximum

Command: vlan mac-address dynamic maximum <*value*>

no vlan mac-address dynamic maximum

Function: Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN; "**no ip mac-address dynamic maximum**" command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Parameters: <*value*> upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address in the VLAN is disabled.

Command Mode: VLAN Configuration Mode.

Usage Guide: When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

Examples: Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.

Switch(config)#vlan1
Switch(Config-if-Vlan1)#vlan mac-address dynamic maximum 50 Enable the number limitation function of dynamic MAC address in VLAN 1
Switch(Config-if-Vlan1)#no vlan mac-address dynamic maximum

43.3 switchport arp dynamic maximum

Command: switchport arp dynamic maximum <*value*>

no switchport arp dynamic maximum

Function: Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; "**no switchport arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP on the port.

Parameters: <*value*> upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic ARP in port 1/2 mode, the max number to be set is 20

Switch(Config-If-Ethernet1/2)#no switchport arp dynamic maximum

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport arp dynamic maximum 20 Disable the number limitation function of dynamic ARP in port 1/2 mode
Switch(Config-If-Ethernet1/2)#no switchport arp dynamic maximum

43.4 switchport nd dynamic maximum

Command: switchport nd dynamic maximum <*value*>

no switchport nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time,

enable the number limitation function of dynamic NEIGHBOR on the port; "**no switchport nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR on the port.

Parameters: <*value*> upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in port 1/2 mode, the max number to be 20.

Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport nd dynamic maximum 20 Disable the number limitation function of dynamic NEIGHBOR in port 1/2 mode
Switch(Config-If-Ethernet1/2)#no switchport nd dynamic maximum

43.5 ip arp dynamic maximum

Command: ip arp dynamic maximum <*value*>

no ip arp dynamic maximum

Function: Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; "**no ip arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP in the VLAN.

Parameters: <*value*> upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP in the VLAN is disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

Examples:

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50

Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ip arp dynamic maximum 50 Disable the number limitation function of dynamic ARP in VLAN 1
Switch(Config-if-Vlan1)#no ip arp dynamic maximum

43.6 ipv6 nd dynamic maximum

Command: ipv6 nd dynamic maximum <*value*>

no ipv6 nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; "**no ipv6 nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Parameters: <*value*> upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50

Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50 Disable the number limitation function of dynamic NEIGHBOR in VLAN 1
Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

43.7 mac-address query timeout

Command: mac-address query timeout <*seconds*>

Function: Set the timeout value of querying dynamic MAC.

Parameter: <*seconds*> is timeout value, in second, ranging from 5 to 300.

Default Settings: Default value is 60 seconds.

Command Mode: Global mode

Usage Guide: After enabling the number limitation of MAC, users can use this command to configure the timeout value of querying dynamic MAC. If the data traffic is very large, the timeout value can be shorter, otherwise, it can be longer. Users can set it according to actual situation.

Examples:

Set the timeout value of quering dynamic MAC as 30 seconds

Switch(config)# mac-address query timeout 30

43.8 show mac-address dynamic count

Command: show mac-address dynamic count { (vlan <1-4096>)| interface ethernet <*portName*>}

Function: Display the number of dynamic MAC of corresponding port and VLAN.

Parameters: <*vlan-id*> display the specified VLAN ID.

<portName> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic MAC of corresponding port and VLAN.

Examples: Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC.

```
Switch(config)# show mac-address dynamic count interface ethernet 1/3
 Port              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/3              5                    1
-------------------------------------------------------------------------------------------------
Switch(config)# show mac-address dynamic count vlan 1
 Vlan              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------------
 1                   55                  15
-------------------------------------------------------------------------------------------------
```

43.9 show arp-dynamic count

Command: show arp-dynamic count { (vlan <1-4096>)| interface ethernet <*portName*>}

Function: Display the number of dynamic ARP of corresponding port and VLAN.

Parameters: <*vlan-id*> is play the specified vlan ID.

<*portName*> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples: Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

```
Switch(config)# show arp-dynamic count interface ethernet 1/3
 Port              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/3              5                    1
-------------------------------------------------------------------------------------------------
Switch(config)# show arp-dynamic count vlan 1
 Vlan              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------------
 1                   55                  15
-------------------------------------------------------------------------------------------------
```

43.10 show nd-dynamic count

Command: show nd-dynamic count {(vlan <1-4096>)| interface ethernet <*portName*>}

Function: Display the number of dynamic ND of corresponding port and VLAN.

Parameters: <*vlan-id*> is play the specified vlan ID. **<*portName*>** is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples: Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND.

```
Switch(config)# show nd-dynamic count interface ethernet 1/3
 Port              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------
 Ethernet1/3              5                    1
-------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic count vlan 1
 Vlan              MaxCount              CurrentCount
-------------------------------------------------------------------------------------------
 1                    55                   15
-------------------------------------------------------------------------------------------
```

43.11 debug switchport mac count

Command: debug switchport mac count

no debug switchport mac count

Function: When the number limitation function debug of MAC on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information." **no debug switchport mac count**" command is used to disable the number limitation function debug of MAC on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic MAC on the port.

Examples:

```
Switch#debug switchport mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet1/1
!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!
```

43.12 debug switchport arp count

Command: debug switchport arp count

no debug switchport arp count

Function: When the number limitation function debug of ARP on the port, if the number of dynamic ARP and the number of ARP on the port is larger than the max number allowed, users will see debug information." **no debug switchport arp count**" command is used to disable the number limitation function debug of ARP on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic ARP on the port.

Examples:

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port Ethernet1/1
!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!
```

43.13 debug switchport nd count

Command: debug switchport nd count

no debug switchport nd count

Function: When the number limitation function debug of ND on the port, if the number of dynamic ND and the number of ND on the port is larger than the max number allowed, users will see debug information." **no debug switchport nd count**" command is used to disable the number limitation function debug of ND on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic ND on the port

Examples:

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in port Ethernet1/1
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!
```

43.14 debug vlan mac count

Command: debug vlan mac count

no debug vlan mac count

Function: When the number limitation function debug of MAC in the VLAN, if the number of dynamic MAC and the number of MAC in the VLAN is larger than the max number allowed, users will see debug information." **no debug vlan mac count**" command is used to disable the number limitation function debug of MAC in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic MAC in the VLAN.

Examples:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!
```

43.15 debug ip arp count

Command: debug ip arp count

no debug ip arp count

Function: When the number limitation function debug of ARP in the VLAN, if the number of dynamic ARP and the number of ARP in the VLAN is larger than the max number allowed, users will see debug information." **no debug ip arp count**" command is used to disable the number limitation function debug of ARP in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic ARP in the VLAN.

Examples:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!
```

43.16 debug ipv6 nd count

Command: debug ipv6 nd count

no debug ipv6 nd count

Function: When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information." **no debug ip neighbor count**" command is used to disable the number limitation function debug of neighbor in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic neighbor in the VLAN.

Examples:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!
```

Chapter 44 Commands for AM Configuration

44.1 am enable

Command: am enable

no am enable

Function: Globally enable/disable AM function.

Parameters: None.

Default: AM function is disabled by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: Enable AM function on the switch.

Switch(config)#am enable Disable AM function on the switch.
Switch(config)#no am enable

44.2 am port

Command: am iport

no am port

Function: Enable/disable AM function on port.

Parameters: None.

Default: AM function is disabled on all port.

Command Mode: Port Mode.

Example: Enable AM function on interface 1/3 of the switch.

Switch(Config-If-Ethernet 1/3)#am port Disable AM function on interface 1/3 of the switch.
Switch(Config-If-Ethernet 1/3)#no am port

44.3 am ip-pool

Command: am ip-pool *<ip-address> <num>*

no am ip-pool *<ip-address> <num>*

Function: Set the AM IP segment of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameters: *<ip-address>* the starting address of an address segment in the IP address pool; ***<num>*** is the number of consecutive addresses following ip-address, less than or equal with 32.

Default: IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that interface 1/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1.

```
Switch(Config-If-Ethernet 1/3)#am ip-pool 10.10.10.1 10
```

44.4 am mac-ip-pool

Command: am mac-ip-pool <*mac-address*> < *ip-address*>

no am mac-ip-pool <*mac-address*> < *ip-address*>

Function: Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameter: <*mac-address*> is the source MAC address; **< *ip-address*>** is the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers.

Default: MAC-IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that the interface 1/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded.

```
Switch(Config-If-Ethernet1/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1
```

44.5 no am all

Command: no am all [ip-pool | mac-ip-pool]

Function: Delete MAC-IP address pool or IP address pool or both pools configured by all users.

Parameters: ip-pool is the IP address pool; **mac-ip-pool** is the MAC-IP address pool; no parameter means both address pools.

Default: Both address pools are empty at the beginning.

Command Mode: Global Mode

Usage Guide: None.

Example: Delete all configured IP address pools.

```
Switch(config)#no am all ip-pool
```

44.6 show am

Command: show am [interface <*interface-name*>]

Function: Display the configured AM entries.

Parameters: <*interface-name*> is the name of the interface of which the configuration information will be displayed. No parameter means to display the AM configuration information of all interfaces.

Command Mode: Admin and Configuration Mode.

Example: Display all configured AM entries.

```
Switch#show am
AM is enabled

Interface Ethernet1/3
        am interface
        am ip-pool 30.10.10.1   20
Interface Ethernet1/5
        am interface
        am ip-pool 50.10.10.1   30
        am mac-ip-pool   00-02-04-06-08-09 20.10.10.5
        am ip-pool 50.20.10.1   20
Interface Ethernet1/6
        am interface
Interface Ethernet1/1
        am interface
        am ip-pool 10.10.10.1   20
        am ip-pool 10.20.10.1   20

Display the AM configuration entries of ehternet1/5 of the switch.
Switch#show am interface ethernet 1/5
AM is enabled

Interface Etherne1/5
        am interface
        am ip-pool 50.10.10.1   30
        am mac-ip-pool   00-02-04-06-08-09 20.10.10.5
    am ip-pool 50.20.10.1   20
```

Chapter 45 Commands for Security Feature

45.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable

Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the “no” form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.

Command Mode: Global Mode

Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped

Example: Drop the data packet whose source IP address is equal to its destination address

Switch(config)# dosattack-check srcip-equal-dstip enable

```
Switch(config)# dosattack-check srcip-equal-dstip enable
```

45.2 dosattack-check ipv4-first-fragment enable

Command: [no] dosattack-check ipv4-first-fragment enable

Function: Enable the function by which the switch checks the first fragment packet of IPv4; the “no” form of this command disables this function.

Parameter: None

Command Mode: Global Mode

Usage Guide: This command has no effect when used separately. It should be used associating dosattack-check tcp-flags enable or dosattack-check srcport-equal-dstport enable command.

Example: Drop the IPv4 fragment or non-fragment data packet whose source port is equal to its destination port.

```
Switch(config)# dosattack-check ipv4-first-fragment enable
```

```
Switch(config)# dosattack-check srcport-equal-dstport enable
```

45.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable

Function: Enable the function by which the switch will check the unauthorized TCP label function; the “no” form of this command will disable this function.

Parameter: None

Default: This function disable on the switch by default

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions

are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command.

Example: Drop one or more types of above four packet types.

```
Switch(config)# dosattack-check tcp-flags enable
```

45.4 dosattack-check srcport-equal-dstport enable

Command: dosattack-check srcport-equal-dstport enable

Function: Enable the function by which the switch will check if the source port is equal to the destination port; the "no" form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch will check if the source port is equal to the destination port.

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port.

Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.

```
Switch(config)# dosattack-check srcport-equal-dstport enable
```

45.5 dosattack-check tcp-fragment enable

Command: [no] dosattack-check tcp-fragment enable

Function: Enable the function by which the switch detects TCP fragment attacks; the “no” form of this command disables this function.

Parameter: None

Default: This function is not enabled on the switch by default

Command Mode: Global Mode

Usage Guide: By enabling this function the switch will be protected from the TCP fragment attacks, dropping the data packets whose TCP fragment offset value is 1 or the TCP head is shorter than the specified value. Use “dosattack-check tcp-header” command to specify the length.

Example: Enable the Checking TCP fragment attack function.e

```
Switch(config)# dosattack-check tcp-fragment enable
```

45.6 dosattack-check tcp-segment

Command: dosattack-check tcp-segment *<20-255>*

Function: Configure the minimum TCP segment length permitted by the switch.

Parameter: <20-255> is the minimum TCP segment length permitted by the switch.

Default: The length is 20 by default which is the shortest TCP segment

Command Mode: Global Mode

Usage Guide: To use this function the “dosattack-check tcp-fragment enable” function must be enabled

Example: Set the minimum TCP segment length permitted by the switch to 20.

```
Switch(config)# dosattack-check tcp-fragment enable
Switch(config)# dosattack-check tcp-segment 20
```

45.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable

Function: Enable the ICMP fragment attack checking function on the switch; the “no” form of this command disables this function.

Parameter: None

Default: Disable the ICMP fragment attack checking function on the switch

Command Mode: Global Mode

Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value.

Example: Enable the ICMP fragment attack checking function.

```
Switch(config)# dosattack-check icmp-attacking enable
```

45.8 dosattack-check icmpv4-size

Command: dosattack-check icmpv4-size <64-1023>

Function: Configure the max net length of the ICMPv4 data packet permitted by the switch.

Parameter: <64-1023> is the max net length of the ICMPv4 data packet permitted by the switch.

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable “dosattack-check icmp-attacking enable” first

Example: Set the max net length of the ICMPv4 data packet permitted by the switch to 100.

```
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpv4-size 100
```

45.9 dosattack-check icmpv6-size

Command: dosattack-check icmpv6-size <64-1023>

Function: Configure the max net length of the ICMPv6 data packet permitted by the switch.

Parameter: <64-1023> is the max net length of the ICMPv6 data packet permitted by the switch.

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable “dosattack-check icmp-attacking enable” first.

Example: Set the max net length of the ICMPv6 data packet permitted by the switch to 100.

```
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpv6-size 100
```

Chapter 46 Commands for TACACS+

46.1 tacacs-server authentication host

Command: tacacs-server authentication host <*ip-address*> [port <*port-number*>] [timeout <*seconds*>] [key <*string*>] [primary]

no tacacs-server authentication host <*ip-address*>

Function: Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the no form of this command deletes TACACS+ authentication server.

Parameter: <*ip-address*> is the IP address of the server;**<*port-number*>** is the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server; **<*seconds*>** is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60; **key <*string*>** is the key string, containing maximum 16 characters; **primary** indicates it's a primary server.

Command Mode: Global Mode

Default: No TACACS+ authentication configured on the system by default.

Usage Guide: This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch. The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout<*seconds*> and key<string>, it will use the global value and key by command tacacs-server timeout<*seconds*> and tacacs-server key <string>. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case **primary** is configured on one TACACS+ server, the server will be the primary server.

Example: Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key.

```
Switch(config)#tacacs-server authentication host 192.168.1.2
```

46.2 tacacs-server key

Command: tacacs-server key <*string*>

no tacacs-server key

Function: Configure the key of TACACS+ authentication server; the "**no tacacs-server key**" command deletes the TACACS+ server key.

Parameter: <*string*> is the character string of the TACACS+ server key, containing maximum 16 characters.

Command Mode: Global Mode

Usage Guide: The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security.

Example: Configure test as the TACACS+ server authentication key.

```
Switch(config)# tacacs-server key test
```

46.3 tacacs-server nas-ipv4

Command: tacacs-server nas-ipv4 <ip-address>

no tacacs-server nas-ipv4

Function: Configure the source IP address of TACACS+ packet sent by the switch; the "**no tacacs-server nas-ipv4**" command deletes the configuration.

Parameter: <ip-address> is the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address.

Default: No specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+ packet.

Command Mode: Global Mode

Usage Guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down.

Example: Configure the source ip address of TACACS+ packet as 192.168.2.254.

```
Switch#tacacs-server nas-ipv4 192.168.2.254
```

46.4 tacacs-server timeout

Command: tacacs-server timeout <*seconds*>

no tacacs-server timeout

Function: Configure a TACACS+ server authentication timeout timer; the "**no tacacs-server timeout**" command restores the default configuration.

Parameter: <*seconds*> is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60.

Command Mode: Global Mode

Default: 3 seconds by default.

Usage Guide: The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed.

Example: Configure the timeout timer of the tacacs+ server to 30 seconds.

```
Switch(config)# tacacs-server timeout 30
```

46.5 debug tacacs-server

Command: debug tacacs-server

no debug tacacs-server

Function: Open the debug message of the TACACS+; the "**no debug tacacs-server**" command closes the TACACS+ debugging messages.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable the TACACS+ debugging messages to check the negotiation process of the TACACS+ protocol which can help detecting the failure.

Example: Enable the debugging messages of the TACACS+ protocol.

```
Switch#debug tacacs-server
```

Chapter 47 Commands for RADIUS

47.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enables the AAA authentication function in the switch; the "no AAA enable" command disables the AAA authentication function.

Command mode: Global Mode.

Parameters: No.

Default: AAA authentication is not enabled by default.

Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.

Example: Enabling AAA function for the switch.

```
Switch(config)#aaa enable
```

47.2 aaa-accounting enable

Command: aaa-accounting enable

no aaa-accounting enable

Function: Enables the AAA accounting function in the switch: the "no aaa-accounting enable" command disables the AAA accounting function.

Command mode: Global Mode

Default: AAA accounting is not enabled by default.

Usage Guide: When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an “accounting started” message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an “accounting stopped” message is sent to the RADIUS accounting server on accounting end. Note: The switch send the “user offline” message to the RADIUS accounting server only when accounting is enabled, the “user offline” message will not be sent to the RADIUS authentication server.

Example: Enabling AAA accounting for the switch.

```
Switch(config)#aaa-accounting enable
```

47.3 aaa-accounting update

Command: **aaa-accounting update {enable|disable}**

Function: Enable or disable the AAA update accounting function.

Command Mode: Global Mode.

Default: Enable the AAA update accounting function.

Usage Guide: After the update accounting function is enabled, the switch will sending accounting message to each online user on time.

Example: Disable the AAA update accounting function for switch.

```
Switch(config) #aaa-accounting update disable
```

47.4 debug aaa packet

Command: debug aaa packet {send|receive|all} interface{ethernet *<interface-number>* | *<interface-name>*}

no debug aaa packet {send|receive|all} interface{ethernet *<interface-number>* | *<interface-name>*}

Function: Enable the debug information of AAA about receiving and sending packets; the no operation of this command will disable such debug information.

Parameters: send: Enable the debug information of AAA about sending packets.

receive: Enable the debug information of AAA about receiving packets.

all: Enable the debug information of AAA about both sending and receiving packets.

***<interface-number>*:** the number of interface.

***<interface-name>*:** the name of interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about sending and receiving packets, users can check the messages received and sent by Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about sending and receiving packets on interface1/1.

```
Switch#debug aaa packet all interface Ethernet 1/1
```

47.5 debug aaa detail attribute

Command: debug aaa detail attribute interface {ethernet *<interface-number>*| *<interface-name>*}

no debug aaa detail attribute interface {ethernet *<interface-number>*| *<interface-name>*}

Function: Enable the debug information of AAA about Radius attribute details; the no operation of this command will disable that debug information.

Parameters: *<interface-number>*: the number of the interface.

***<interface-name>*:** the name of the interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about Radius attribute details, users can check Radius attribute details of Radius messages, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about Radius attribute details on interface 1/1.

```
Switch#debug detail attribute interface Ethernet 1/1
```

47.6 debug aaa detail connection

Command: debug aaa detail connection

no debug aaa detail connection

Function: Enable the debug information of AAA about connection details; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about connection details, users can check connection details of AAA, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about connection details.

```
Switch#debug aaa detail connection
```

47.7 debug aaa detail event

Command: debug aaa detail event

no debug detail event

Function: Enable the debug information of AAA about events; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about events, users can check the information of all kinds of event generated in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about events.

```
Switch#debug aaa detail event
```

47.8 debug aaa error

Command: debug aaa error

no debug error

Function: Enable the debug information of AAA about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of AAA about errors, users can check the information of all kinds of errors that occurs in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of AAA about errors.

```
Switch#debug aaa error
```

47.9 radius nas-ipv4

Command: radius nas-ipv4 *<ip-address>*

no radius nas-ipv4

Function: Configure the source IP address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command deletes the configuration.

Parameter: *<ip-address>* is the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address.

Default: No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.

Command mode: Global Mode.

Usage guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ip address of RADIUS packet as 192.168.2.254.

```
Switch#radius nas-ipv4 192.168.2.254
```

47.10 radius nas-ipv6

Command: radius nas-ipv6 *<ipv6-address>*

no radius nas-ipv6

Function: Configure the source IPv6 address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command deletes the configuration.

Parameter: *<ipv6-address>* is the source IPv6 address of the RADIUS packet, it mast be a valid unicast IPv6 address.

Default: No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.

Command mode: Global Mode.

Usage guide: The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1.

```
Switch#radius nas-ipv6 2001:da8:456::1
```

47.11 radius-server accounting host

Command: radius-server accounting host {*<ipv4-address>*|*<ipv6-address>*} [port <port-number>] [primary]

no radius-server accounting host {*<ipv4-address>*|*<ipv6-address>*}

Function: Specifies the IPv4/IPv6 address and listening port number for RADIUS accounting server; the no command deletes the RADIUS accounting server.

Parameters: ***<ipv4-address>*|*<ipv6-address>*** stands for the server IPv4/IPv6 address; ***<port-number>*** for server listening port number from 0 to 65535;

primary for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used first.

Command Mode: Global Mode

Default: No RADIUS accounting server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The

<port-number> parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If **primary** is specified, then the specified RADIUS server will be the primary server.

Example: Sets the RADIUS accounting server of IP address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000.

```
Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary
```

47.12 radius-server authentication host

Command: radius-server authentication host {*<ipv4-address >|<ipv6-address>*} [port <port-number>] [key <*string*>] [primary] [access-mode {dot1x|telnet}]

no radius-server authentication host {*<ipv4-address >|<ipv6-address>*}

Function: Specifies the IP address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no command deletes the RADIUS authentication server.

Parameters: *<ipv4-address >|<ipv6-address>* stands for the server IPv4/IPv6 address;

<port-number> for listening port number, from 0 to 65535, where 0 stands for non-authentication server usage;

<string> is cipher key string;

primary for primary server. Multiple RADIUS Sever can be configured and would be available. RADIUS Server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used last.

[access-mode {dot1x|telnet}] designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default.

Command mode: Global Mode

Default: No RADIUS authentication server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is successed or failed), switch does not send the authentication request to the next. If **primary** is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by **radius-server key <string>** global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

Example: Setting the RADIUS authentication server address as 2004:1:2:3::2.

```
Switch(config)#radius-server authentication host 2004:1:2:3::2
```

47.13 radius-server dead-time

Command: radius-server dead-time <*minutes*>

no radius-server dead-time

Function: Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.

Parameters: < *minute* > is the down -restore time for RADIUS server in minutes, the valid range is 1 to 255.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid.

Example: Setting the down-restore time for RADIUS server to 3 minutes.

```
Switch(config)#radius-server dead-time 3
```

47.14 radius-server key

Command: radius-server key <*string*>

no radius-server key

Function: Specifies the key for the RADIUS server (authentication and accounting); the "no radius-server key" command deletes the key for RADIUS server.

Parameters: <*string*> is a key string for RADIUS server, up to 16 characters are allowed.

Command mode: Global Mode

Usage Guide: The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.

Example: Setting the RADIUS authentication key to be "test".

```
Switch(config)# radius-server key test
```

47.15 radius-server retransmit

Command: radius-server retransmit <*retries*>

no radius-server retransmit

Function: Configures the re-transmission times for RADIUS authentication packets; the "**no radius-server retransmit**" command restores the default setting.

Parameters: <*retries*> is a retransmission times for RADIUS server, the valid range is 0 to 100.

Command mode: Global Mode

Default: The default value is 3 times.

Usage Guide: This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid.

Example: Setting the RADIUS authentication packet retransmission time to five times.

```
Switch(config)# radius-server retransmit 5
```

47.16 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configures the timeout timer for RADIUS server; the "**no radius-server timeout**" command restores the default setting.

Parameters: <*seconds*> is the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000.

Command mode: Global Mode

Default: The default value is 3 seconds.

Usage Guide: This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions.

Example: Setting the RADIUS authentication timeout timer value to 30 seconds.

```
Switch(config)# radius-server timeout 30
```

47.17 radius-server accounting-interim-update timeout

Command: radius-server accounting-interim-update timeout <*seconds*>

no radius-server accounting-interim-update timeout

Function: Set the interval of sending fee-counting update messages; the no operation of this command will reset to the default configuration.

Parameters: <*seconds*> is the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600.

Command Mode: Global Mode.

Default: The default interval of sending fee-counting update messages is 300 seconds.

User Guide: This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

The recommended ratio of the interval of sending fee-counting update messages to the maximum number of the users supported by NAS

The maximum number of users The interval of sending fee-counting update messages(in seconds)
1~299 300（default value）
300~599 600
600~1199 1200
1200~1799 1800
≥1800 3600

Example: The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.

```
Switch(config)#radius-server accounting-interim-update timeout 1200
```

47.18 show aaa authenticated-user

Command: show aaa authenticated-user

Function: Displays the authenticated users online.

Command mode: Admin and Configuration Mode.

Usage Guide: Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.

Example:

```
witch#show aaa authenticated-user
------------------------- authenticated users -------------------------------
 UserName   Retry RadID Port EapID ChapID OnTime      UserIP            MAC
-----------------------------------------------------------------------------


              ---------- total: 0 ----------
```

47.19 show aaa authenticating-user

Command: show aaa authenticating-user

Function: Display the authenticating users.

Command mode: Admin and Configuration Mode.

Usage Guide: Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.

Example:

```
Switch#show aaa authenticating-user

------------------------ authenticating users -----------------------------
    User-name     Retry-time   Radius-ID     Port   Eap-ID Chap-ID Mem-Addr     State
-------------------------------------------------------------------------------

               ---------- total: 0 ----------
```

47.20 show aaa config

Command: show aaa config

Function: Displays the configured commands for the switch as a RADIUS client.

Command mode: Admin and Configuration Mode.

Usage Guide: Displays whether AAA authentication, accounting are enabled and information for key, authentication and accounting server specified.

Example:

```
Switch#show aaa config（For Boolean value, 1 stands for TRUE and 0 for FALSE）

----------------- AAA config data ------------------

      Is Aaa Enabled = 1        :1 means AAA authentication is enabled, 0 means is not enabled
      Is Account Enabled= 1     :1 means AAA account is enabled, 0 means is not enabled
      MD5 Server Key = yangshifeng     : Authentication key
      authentication server sum = 2        :Configure the number of authentication server
      authentication server[0].sock_addr = 2:100.100.100.60.1812   :The address protocol
group, IP and interface number of the first authentication server
                                    .Is Primary = 1        :Is the primary server
                                    .Is Server Dead = 0   :The server whether dead
                                    .Socket No = 0   :The local socket number lead to this server
      authentication server[1].sock_addr = 10:2004:1:2::2.1812
                                    .Is Primary = 0
                                    .Is Server Dead = 0
                                    .Socket No = 0
      accounting server sum = 2   :Configure the number of the accounting server
      accounting server[0].sock_addr = 2:100.100.100.65.1813   :The address protocol group,
```

```
IP and interface number of the accounting server
                                    .Is Primary = 1       :Is primary server
                                    .Is Server Dead = 0   :This server whether dead
                                    .Socket No = 0    :The local socket number lead to this
server
      accounting server[1].sock_addr = 10:2004::7.1813
                                    .Is Primary = 1
                                    .Is Server Dead = 0
                                    .Socket No = 0
     Time Out = 5s   :After send the require packets, wait for response time out
     Retransmit = 3   :The number of retransmit
     Dead Time = 5min   :The tautology interval of the dead server
      Account Time Interval = 0min   :The account time interval
```

47.21 show radius count

Command: show radius {authenticated-user|authenticating-user} count

Function: Displays the statistics for users of RADIUS authentication.

Parameters: authenticated-user displays the authenticated users online; **authenticating-user** displays the authenticating users.

Command mode: Admin and Configuration Mode.

Usage Guide: The statistics for RADIUS authentication users can be displayed with the "**show radius count**" command.

Example:

1. Display the statistics for RADIUS authenticated users.

```
Switch #show radius authenticated-user count
The authenticated online user num is:        0
```

2. Display the statistics for RADIUS authenticated users and others.

```
Switch #sho radius authenticating-user count
```

Chapter 48 Commands for SSL Configuration

48.1 ip http secure-server

Command: ip http secure-server

no ip http secure-server

Function: Enable/disable SSL function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication.

Example: Enable SSL function.

```
Switch(config)# ip http secure-server
```

48.2 ip http secure-port

Command: ip http secure-port <*port-number*>

no ip http secure-port

Function: Configure/delete port number by SSL used.

Parameter: <*port-number*> means configured port number, range between 1025 to 65535. 443 is for default.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example: https://device:port_number. SSL function must reboot after every change.

Example: Configure the port number is 1028.

```
Switch(config)# ip http secure-port 1028
```

48.3 ip http secure- ciphersuite

Command: ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}

no ip http secure-ciphersuite

Function: Configure/delete secure cipher suite by SSL used.

Parameter: des-cbc3-sha encrypted algorithm DES_CBC3，summary algorithm SHA.

rc4-128-sha encrypted algorithm RC4_128，summary algorithm SHA.

des-cbc-sha encrypted algorithm DES_CBC，summary algorithm SHA.

default use is **rc4-md5**.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration. When des-cbc-sha is configured, IE 7.0 or above is required.

Example: Configure the secure cipher suite is rc4-128-sha.

```
Switch(config)# ip http secure- ciphersuite rc4-128-sha
```

48.4 show ip http secure-server status

Command: show ip http secure-server status

Function: Show the status for the configured SSL.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha
```

48.5 debug ssl

Command: debug ssl

no debug ssl

Function: Show the configured SSL information, the no command closes the DEBUG.

Parameter: None.

Command Mode: Admin Mode.

Example:

```
Switch# debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server success!
```

Chapter 49 Commands for IPv6 Security RA

49.1 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. The no operation of this command will globally disable IPv6 security RA function.

Parameters: None.

Command Mode: Global Configuration Mode.

Default: The IPv6 security RA function is disabled by default.

Usage Guide: Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

Example: Globally enable IPv6 security RA.

```
Switch(config)#ipv6 security-ra enable
```

49.2 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Enable IPv6 security RA on a port, causing this port not to forward the received RA message. The **no ipv6 security-ra enable** will disable the IPv6 security RA on a port.

Parameters: None.

Command Mode: Port Configuration Mode.

Default: IPv6 security RA function is disabled by default.

Usage Guide: Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

Example: Enable IPv6 security RA on a port.

```
Switch(Config-If-Ethernet1/2)#ipv6 security-ra enable
```

49.3 show ipv6 security-ra

Command: show ipv6 security-ra [interface *<interface-list>*]

Function: Display all the interfaces with IPv6 RA function enabled.

Parameters: No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
```

```
Ethernet1/1
IPv6 Security RA State: Yes
Ethernet1/3
IPv6 Security RA State: Yes
```

49.4 debug ipv6 security-ra

Command: debug ipv6 security-ra

no debug ipv6 security-ra

Function: Enable the debug information of IPv6 security RA; the no operation of this command will disable the debug information of IPv6 security RA.

Command Mode: Admin Mode.

Parameters: None.

Usage Guide: Users can check the proceeds of message handling of IPv6 security RA, which will help investigate the causes to problems if there is any.

Example: Enable the debug information of IPv6 security RA.

```
Switch#debug ipv security-ra
```

Chapter 50 Commands for VLAN-ACL

50.1 clear vacl statistic vlan

Command: clear vacl [in | out] statistic vlan [<*1-4094*>]

Function: This command can clear the statistic information of VACL.

Parameter: in | out: Clear the traffic statistic of the ingress/egress.

vlan <*1-4094*>: The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information.

Command mode: Admin Mode.

Default: None.

Usage Guide: None.

Example:

Clear VACL statistic information of Vlan1.

```
Switch# clear vacl statistic vlan 1
```

50.2 show vacl vlan

Command: show vacl [in | out] vlan [<*1-4094*>] | [begin | include | exclude <*regular-expression*>]

Function: This command shows the configuration and the statistic information of VACL.

Parameter: in | out: Show ingress/egress configuration and statistic

vlan <*1-4094*>: The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.

begin | include | exclude <*regular-expression*>: the regular expression

. match any characters except the line feed character

^ match the beginning of the row

$ match the end of the row

| match the character string at the left or right of upright line

[0-9] match the number 0 to the number 9

[a-z] match the lowercase a to z

[aeiou] match any letter in “aeiou”

\ Escape Character is used to match the intervocalic character, for example, \$ will match the $ character, but it is not match the end of the character string

\w match the letter, the number or the underline

\b match the beginning or the end of the words

\W match any characters which are not alphabet letter, number and underline

\B match the locations which are not the begin or end of the word

[^x] match any characters except x

[^aeiou] match any characters except including aeiou letters

* repeat zero time or many times

+ repeat one time or many times

(n) repeat n times

(n,) repeat n or more times

(n, m) repeat n to m times

At present, the regular expression used does not support the following syntaxes:

\s match the blank character

\d match the number

\S match any characters except blank character

\D match non-number character

? repeat zero time or one time

Command mode: Admin Mode.

Default: None.

Usage Guide: None.

Example:

Switch (config)#show vacl vlan 2 Vlan 2: IP Ingress access-list used is 100, traffic-statistics Disable.
Switch (config)# show vacl vlan 3 Vlan 3: IP Ingress access-list used is myacl, packet(s) number is 5.

Displayed Information Explanation
Vlan 2 The name of VLAN
100, myacl The name of VACL
traffic-statistics Disable Disable VACL statistic function
packet(s) number is 5 The sum of out-profile data packets matching this VACL

50.3 vacl ip access-group

Command: vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD

Function: This command configure VACL of IP type on the specific VLAN.

Parameter: <1-299> | WORD: Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters.

Example: Configure the numeric IP ACL and enable the statistic function for Vlan 1-5, 6, 7-9.

```
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9
```

50.4 vacl ipv6 access-group

Command: vacl ipv6 access-group (<500-699> | WORD) {in | out} (traffic-statistic|) vlan WORD

no ipv6 access-group {<500-699> | WORD} {in | out} vlan WORD

Function: This command configure VACL of IPv6 on the specific VLAN.

Parameter: <500-699> | WORD: Configure the numeric IP ACL (include: IPv6 standard ACL rule <500-599>, IPv6 extended ACL rule <600-699>) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters.

Example: Configure the numeric IPv6 ACL for Vlan 5.

```
Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5
```

50.5 vacl mac access-group

Command: vacl mac access-group {<700-1199> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl mac access-group {<700-1199> | WORD} {in | out} vlan WORD

Function: This command configure VACL of MAC type on the specific VLAN.

Parameter: <700-1199> | WORD: Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters.

Example: Configure the numeric MAC ACL for Vlan 1-5.

```
Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5
```

50.6 vacl mac-ip access-group

Command: vacl mac-ip access-group {<3100-3299> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl mac-ip access-group {<3100-3299> | WORD} {in | out} vlan WORD

Function: This command configure VACL of MAC-IP type on the specific VLAN.

Parameter: <3100-3299> | WORD: Configure the numeric IP ACL or the named ACL.

in | out: Filter the ingress/egress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length can not exceed 80 characters.

Example: Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.

```
Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5
```

Chapter 51 Commands for Mirroring Configuration

51.1 monitor session source interface

Command: monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]} {rx| tx| both}

no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}

Function: Specify the source interface for the mirror. The no form command will disable this configuration.

Parameters: <*session*> is the session number for the mirror. Currently only 1 to 4 is supported. **<*interface-list*>** is the list of source interfaces of the mirror which can be separated by "-"and ";". **cpu** slot <slotnum> specifies the CPU on the specified board to be the source of the mirror for debugging. Datagram received by or/and sent by the specified CPU. Currently the CPU mirror is only supported be configured in session 4. **rx** means to filter the datagram received by the interface, while **tx** for the datagram sent out, and **both** means both of income and outcome datagram.

Command mode: Global mode

Usage Guide: This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. Both of the income and outcome datagram can be mirrored, or they can be mirrored selectively. If no [rx | tx | both] is specified, both are made to be the default. When multiple interfaces are mirrored, the direction of the mirror can be different, but they should be configured separately.

Example: Configure to mirror the datagram sent out by interface 1/1-4, and to mirror the datagram received by interface 1/5.

Switch(config)#monitor session 1 source interface ethernet 1/1-4 rx
Switch(config)#monitor session 1 source interface ethernet 1/5 rx

51.2 monitor session source interface access-list

Command: monitor session <*session*> source {interface <*interface-list*>} access-list <*num*> {rx | tx | both}

no monitor session <*session*> source {interface <*interface-list*>} access-list <*num*>

Function: Specify the access control for the source of the mirror. The no form command will disable this configuration.

Parameters: <*session*> is the session number for the mirror. Currently only 1 to 4 is supported. **<*interface-list*>** is the list of source interfaces of the mirror which can be separated by "-" and ";". **<*num*>** is the number of the access list. **rx** means to filter the datagram received by the interface. **tx** for the datagram sent out, and **both** means both of income and outcome datagram.

Command Mode: Global Mode.

Usage Guide: This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple

interfaces. For flow mirror, only datagram received can be mirrored. The parameters can be **rx, tx, both**. The related access list should be prepared before this command is issued. For how to configure the access list, please refer to ACL configuration. The mirror can only be created after the destination interface of the corresponding session has been configured.

Example: Configure the mirror interface 1/6 to filter with access list 120 in session 2.

```
Switch(config)#monitor session 2 source interface 1/6 access-list 120 rx
```

51.3 monitor session destination interface

Command: monitor session <*session*> destination interface <*interface-number*>

no monitor session <*session*> destination interface <*interface-number*>

Function: Specify the destination interface of the mirror. The no form command will disable this configuration.

Parameters: <*session*> is the session number of the mirror, which is currently limited to 1-4. **<*interface-number*>** is the destination interface of the mirror.

Default: None.

Command Mode: Global mode

Usage Guide: 4 destination mirror interface is supported on the switch. To be mentioned. The interface which is configured as the destination of the mirror should not be configured as the member of the interface trunk. And the maximum throughput of the interface is recommended to be larger than the total throughput of the interfaces to be mirrored. If the destination of a session is removed, the mirror path configured in the session will be removed at the same time. And if the destination interface is reconfigured, the interface, CPU and mirror path will be recovered. To be mentioned, the flow mirror can only be recovered after the destination of the interface is re-configured.

Example: Configure interface 1/7 as the destination of the mirror.

```
Switch(config)#monitor session 1 destination interface ethernet 1/7
```

51.4 show monitor

Command: show monitor

Function: To display information about the source and destination ports of all the mirror sessions.

Command Mode: Admin Mode

Usage Guide: This command is used to display the source and destination ports for the configured mirror sessions. For port mirroring, CPU mirroring, and flow mirroring, the mirror mode of the source can be displayed. For MAC mirroring, MAC mirror configuration will be displayed for the supported switch cards.

Example:

```
Switch#show monitor
```

Chapter 52 Commands for RSPAN Configuration

52.1 remote-span

Command: remote-span

no remote-span

Function: To configure VLAN to RSPAN VLAN. The no form of this command will delete the RSPAN VLAN.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Not configured.

Usage Guide: This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN, should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.

Example:

```
Switch(Config-Vlan5)#remote-span
```

52.2 monitor session remote vlan

Command: monitor session <*session*> remote vlan <*vid*>

no monitor session <*.session*> remote vlan

Function: To configure local mirror session to RSPAN. The no form of this command will restore the RSPAN to local mirror.

Parameter: <*session*>: session ID ，range between 1 to 4. **<*vid*>:** The id of RSPAN VLAN.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.

Example:

```
Switch(config)#monitor session 1 remote vlan 5
```

52.3 monitor session reflector-port

Command: monitor session <*session*> reflector-port <*interface-number*>

no monitor session <*session*> reflector-port <*interface-number*>

Function: To configure reflector port, the no form of this command will delete the reflector port.

Parameter: <*session*>: Session ID, range between 1 to 4, **<*interface-number*>:** Interface number.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN.

Example:

```
Switch(config)#monitor session 1 reflector-port ethernet1/3
```

Chapter 53 Commands for sFlow

53.1 sflow destination

Command: sflow destination <*collector-address*> [<*collector-port*>]

no sflow destination

Function: Configure the IP address and port number of the host on which the sFlow analysis software is installed. If the port has been configured with IP address, the port configuration will be applied, or else the global configuration will be applied. The “no” form of this command restores the port to default and deletes the IP address.

Parameter: <*collector-address*> is the IP address of the analyzer, shown in dotted decimal notation. **<*collector-port*>** is the destination port of the sent sFlow packets.

Command Mode: Global Mode and Port Mode.

Default: The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.

Usage Guide: If the analyzer address is configured at Port Mode, this IP address and port configured at Port Mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.

Example: Configure the analyzer address and port at global mode.

```
switch (config)#sflow destination 192.168.1.200 1025
```

53.2 sflow agent-address

Command: sflow agent-address <*agent-address*>

no sflow agent-address

Function: Configure the sFlow sample proxy address. The “no” form of this command deletes the proxy address.

Parameter: <*agent-address* > is the sample proxy IP address which is shown in dotted decimal notation.

Command Mode: Global Mode.

Default: None default value.

Usage Guide: The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.

Example: Sample the proxy address at global mode.

```
switch (config)#sflow agent-address 192.168.1.200
```

53.3 sflow priority

Command: sflow priority <*priority-value*>

no sflow priority

Function: Configure the priority when sFlow receives packet from the hardware. The "no” form of the command restores to the default.

Parameter: <*priority-value*> is the priority value with a valid range of 0-3.

Command Mode: Global Mode.

Default: The default value is 0.

Usage Guide: When sample packet is sent to the CPU, it is recommended not to assign high priority for the packet so that regular receiving and sending of other protocol packet will not be interfered. The higher the priority value is set, the higher its priority will be.

Example: Configure the priority when sFlow receives packet from the hardware at global mode.

```
switch (config)#sflow priority 1
```

53.4 sflow header-len

Command: sflow header-len *<length-value>*

no sflow header-len

Function: Configure the length of the head data packet copied in the sFlow data sampling. The “no” form of this command restores to the default value.

Parameter: *<length-value>* is the value of the length with a valid range of 32-256.

Command Mode: Port Mode.

Default: 128 by default.

Usage Guide: If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command.

Example: Configure the length of the packet data head copied in the sFlow data sampling to 50.

```
Switch(Config-If-Ethernet1/2)#sflow header-len 50
```

53.5 sflow data-len

Command: sflow data-len *<length-value>*

no sflow data-len

Function: Configure the max length of the sFlow packet data; the “**no sflow data-len**” command restores to the default value.

Parameter: *<length-value>* is the value of the length with a value range of 500-1470.

Command Mode: Port Mode.

Default: The value is 1400 by default.

Usage Guide: When combining several samples to a sFlow group to be sent, the length of the group excluding the MAC head and IP head parts should not exceed the configured value.

Example: Configure the max length of the sFlow packet data to 1000.

```
switch (Config-If-Ethernet1/2)#sflow data-len 1000
```

53.6 sflow counter-interval

Command: sflow counter-interval *<interval-value>*

no sflow counter-interval

Function: Configure the max interval of the sFlow statistic sampling; the “no” form of this command deletes the statistic sampling interval value.

Parameter:*<interval-value>* is the value of the interval with a valid range of 20~120 and shown in second.

Command Mode: Port Mode

Default: No default value

Usage Guide: If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.

Example: Set the statistic sampling interval on the interface e1/1 to 20 seconds.

```
Switch(Config-If-Ethernet1/1)#sflow counter-interval 20
```

53.7 sflow rate

Command: sflow rate { input *<input-rate>* | output *<output-rate* >}

no sflow rate [input | output]

Function: Configure the sample rate of the sFlow hardware sampling. The “no” form of this command deletes the sampling rate value.

Parameter: *<input-rate>* is the rate of ingress group sampling, the valid range is 1000~16383500.

<output-rate> is the rate of egress group sampling, the valid range is 1000~16383500.

Command Mode: Port Mode.

Default: No default value.

Usage Guide: The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.

Example: Configure the ingress sample rate on port e1/1 to 10000 and the egress sample rate to 20000.

```
Switch(Config-If-Ethernet1/1)#sflow rate input 10000
```

```
Switch(Config-If-Ethernet1/1)#sflow rate output 20000
```

53.8 show sflow

Command: show sflow

Function: Display the sFlow configuration state.

Parameter: None.

Command Mode: All Modes.

Usage Guide: This command is used to acknowledge the operation state of sFlow.

```
Switch#show sflow
Sflow version 1.2
Agent address is 172.16.1.100
Collector address have not configured
Collector port is 6343
Sampler priority is 2
Sflow DataSource: type 2, index 194(Ethernet1/2)
   Collector address is 192.168.1.200
   Collector port is 6343
```

```
Counter interval is 0
Sample rate is input 0, output 0
Sample packet max len is 1400
Sample header max len is 50
Sample version is 4
```

Displayed Information Explanation
Sflow version 1.2 Indicates the sFlow version is 1.2
Agent address is 172.16.1.100 Address of the sFlow sample proxy is 172.16.1.100
Collector address have not configured the sFlow global analyzer address is not configured
Collector port is 6343 the sFlow global destination port is the defaulted 6343
Sampler priority is 2 The priority of sFlow when receiving packets from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/1) One sample proxy data source of the sFlow is the interface e1/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200 The analyzer address of the sampling address of the E1/1 interface is 192.168.1.200
Collector port is 6343 Default value of the port on E1/1 interface sampling proxy is 6343.
Counter interval is 20 The statistic sampling interval on e1/1 interface is 20 seconds
Sample rate is input 10000, output 0 The ingress traffic rate of e1/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed
Sample packet max len is 1400

The length of the sFlow group data sent by the e1/1 interface should not exceed 1400 bytes.
Sample header max len is 50 The length of the packet data head copied in the data sampling of the e1/1 interface sampling proxy is 50
Sample version is 4 The datagram version of the sFlow group sent by the E1/1 interface sampling proxy is 4.

Chapter 54 Commands for VRRP

54.1 advertisement-interval

Commands: advertisement-interval <*adver_interval*>

no advertisement-interval

Function: Sets the vrrp timer values; the **"no advertisement-interval"** command restores the default setting.

Parameters: <*adver_interva*> is the interval for sending VRRP packets in seconds, ranging from 1 to 10.

Default: The default **<*adver_interva*>** is 1second.

Command mode: VRRP protocol configuration mode

Usage Guide: The Master in a VRRP Standby cluster will send VRRP packets to member routers (or L3 Ethernet switch) to announce its properness at a specific interval; this interval is referred to as *adver_interval*. If a Backup does not receive the VRRP packets sent by the Master after a certain period (specified by *master_down_interval*), then it assume the Master is no longer operating properly, therefore turns its status to Master.

The user can use this command to adjust the VRRP packet sending interval of the Master. For members in the same Standby cluster, this property should be set to a same value. To Backup, the value of *master_down_interval* is three times that of adver_interval. Extraordinary large traffic or timer setting differences between routers (or L3 Ethernet switches) may result in *master_down_interval* and invoke instant status changes. Such situations can be avoided through extending *adver_interval* interval and setting longer preemptive delay time.

Example: Configuring vrrp Timer value to 3

```
Switch(Config-Router-Vrrp)# advertisement-interval 3
```

54.2 circuit-failover

Commands: circuit-failover {IFNAME | ethernet IFNAME | Vlan <ID>} <value_reduced>

no circuit-failover

Function: Configures the VRRP monitor interface.

Parameters: < *IFNAME* > is the name for the interface to be monitored.

<*value_reduced*> stands for the amount of priority decreased, the default value is 1~253.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRP to provide failover function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is down.

When this command is used, if the status of an interface monitored turns from up to down, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease, lest Backup cannot changes its status due to lower priority than the Master when the Master fails.

Example: Configuring VRRP monitor interface to vlan 2 and decreasing amount of priority to 10.

```
Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10
```

54.3 debug vrrp

Commands: debug vrrp [all | event | packet [recv | send]]

no debug vrrp [all | event | packet [recv | send]]

Function: Displays information for VRRP standby cluster status and packet transmission; the **"no**

debug vrrp" command disables the debug information.

Default: Debugging information is disabled by default.

Command mode: Admin Mode

Example:

```
Switch#debug vrrp
2001/01/01 00:50:28 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:30 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:31 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:32 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
2001/01/01 00:50:33 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]
```

54.4 disable

Commands: disable

Function: Deactivates VRRP

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Deactivates a Virtual Router. VRRP configuration can only be modified when VRRP is deactivated.

Example: Deactivating a Virtual Router numbered as 10.

```
Switch(config)# router vrrp 10
```

```
Switch(Config-Router-Vrrp)#disable
```

54.5 enable

Commands: enable

Function: Activates VRRP.

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Activates the appropriate Virtual Router. Only a router (or L3 Ethernet switch) interface started by this enable command is part of Standby cluster. VRRP virtual IP and interface must be configured first before starting Virtual Router.

Example: Activating the Virtual Router of number 10.

```
Switch(config)#router vrrp 10
```

```
Switch(Config-Router)#enable
```

54.6 interface

Commands: interface {IFNAME | Vlan <*ID*>}

no interface

Function: Configures the VRRP interface.

Parameters: IFNAME: Interface name, for example “VLAN1”.

Vlan <*ID*>: VLAN ID.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a layer 3 interface to an existing Standby cluster. The "**no interface**" command removes the L3 interface from the specified Standby cluster.

Example: Configuring the interface as "interface vlan 1".

```
Switch(config-router)#router vrrp 10
```

```
Switch(Config-router)#interface vlan 1
```

54.7 preempt-mode

Commands: preempt-mode {true | false}

Function: Configures the preemptive mode for VRRP.

Parameters: N/A.

Command mode: VRRP protocol configuration mode

Default: Preemptive mode is set by default.

Usage Guide: If a router (or L3 Ethernet switch) requiring high priority needs to preemptively become the active router (or L3 Ethernet switch), the preemptive mode should be enabled.

Example: Setting non-preemptive VRRP mode.

```
Switch(Config-Router-Vrrp)#preempt-mode false
```

54.8 priority

Commands: priority <*value*>

Function: Configures VRRP priority.

Parameters: <*value*> is the priority value, ranging from 1 to 254.

Default: The priority of all backup routers (or L3 Ethernet switch) in a Standby cluster is 100.

Command mode: VRRP protocol configuration mode

Usage Guide: Priority determines the ranking of a router (or L3 Ethernet switch) in a Standby cluster, the higher priority the more likely to become the Master. When a router (or L3 Ethernet switch) is configured as Master dummy IP address, its priority is always 254 and does not allow modification. When 2 or more routers (or L3 Ethernet switch) with the same priority value present in a Standby cluster, the router (or L3 Ethernet switch) with the greatest VLAN interface IP address becomes the Master.

Example: Setting VRRP priority to 150.

```
Switch(Config-Router-Vrrp)# priority 150
```

54.9 router vrrp

Commands: router vrrp <*vrid*>

no router vrrp <*vrid*>

Function: Creates/Removes the Virtual Router.

Parameters: <*vrid*> is the Virtual Router number ranging from 1 to 255.

Default: Not configured by default.

Command mode: Global Mode

Usage Guide: This command is used to create/remove Virtual Router, which is identified by a unique Virtual Router number. Virtual Router configurations are only available when a Virtual Router is created.

Example: Configuring a Virtual Router with number 10.

```
Switch(config)# router vrrp 10
```

54.10 show vrrp

Commands: show vrrp [<*vrid*>]

Function: Displays status and configuration information for the VRRP standby cluster.

Parameters: < *vrid* > is the Virtual Router number ranging from 1 to 255.

Command mode: Admin and Configuration Mode.

Usage Guide: This command is used to display the Virtual Router configuration and current state. If not specified the Virtual Router number, then display all Virtual Router information.

Example:

```
Switch# show vrrp
  VrId <1>
  State is Initialize
  Virtual IP is 10.1.20.10 (Not IP owner)
  Interface is Vlan1
  Priority not configured, Current priority is 254
  Advertisement interval is 1 sec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 1, Status UP
VrId <10>
  State is Initialize
  Virtual IP is1.1.1.1 (Not IP owner)
  Interface is unset
  Priority is unset
  Advertisement interval is unset
Preempt mode is TRUE
```

```
Switch#
```

Displayed information Explanation
State Status
Virtual IP Dummy IP address
Interface Interface Name
Priority Priority
Advertisement interval Timer interval
Preempt Preemptive mode
Circuit failover interface Interface Monitor information

54.11 virtual-ip

Commands: virtual-ip *<A.B.C.D>*

no virtual-ip

Function: Configures the VRRP dummy IP address.

Parameters: *<A.B.C.D>* is the IP address in decimal format.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a dummy IP address to an existing Standby cluster. The "**no virtual-ip**" command removes the dummy IP address from the specified Standby cluster. Each Standby cluster can have only one dummy IP. VRRP priority as 255 (not configure), virtual-ip and interface ip should in the same segment.
Special Notice: When updating to the newest version from 5.2.0.0 or an older one, the original VRRP command configuration can't be restored. Please delete the original configuration with "no router vrrp <vrid>", and then reconfigure. Otherwise, problems like suspended tasks may happen.

Example: Setting the backup dummy IP address to 10.1.1.1.

```
Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1
```

Chapter 55 Commands for IPv6 VRRPv3 Configuration

55.1 advertisement-interval

Command: advertisement-interval <*adver_interval*>

Function: Configure the advertisement interval of VRRPv3.

Parameters: <*adver_interval*> is the interval of sending VRRPv3 advertisement messages, in centiseconds, ranging from 100 to 1000, and has to be a multiple of 100.

Command Mode: VRRPv3 Protocol Mode.

Default: <*adver_interval*> is 100 centiseconds (1 second) by default.

Usage Guide: The Master in a VRRPv3 backup group will send a VRRPv3 message to notify other routers (layer-three switches) in the group that it is working normally at intervals. This interval is ***adver_interval***. If the Backup hasn't received any VRRPv3 message from Master over a certain period of time (the length of the time is ***master_down_interval***), it will assume that the master is not working normally and will change the state of itself to Master.

Uses can use this command to adjust the interval of VRRPv3 advertisement messages sent by Master. For the members in the same backup group, this attribute should have same value. For Backup, the value of its ***master_down_interval*** should be three times more than *adver_interval*. If the network flow is too big or different routers (or layer-three switches) have different timers, ***master_down_interval*** might has a time-out, which will cause a state change as a result. This kind of situation can be solved by prolonging ***adver_interval*** or setting a longer preempts delay time.

Example: Configure the VRRPv3 advertisement interval as 300 centiseconds.

```
Switch(config-router)# advertisement-interval 300
```

55.2 circuit-failover

Commands: circuit-failover {vlan<*ID*>| *IFNAME*} <*value_reduced*>

no circuit-failover

Function: Configures the VRRPv3 monitor interface.

Parameters: {vlan<*ID*>| *IFNAME*} is the name for the interface to be monitored.

<*value_reduced*> stands for the amount of priority decreased, the range value is from 1 to 253.

Command mode: VRRPv3 Protocol Configuration Mode.

Default: Not configured by default.

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRPV3 to provide backup function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is **down**.

When this command is used, if the status of an interface monitored turns from **up** to **down**, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease (If the priority of that value_reduced is higher than interface configuration, then the corresponding router is **down**, the priority of interface in Backup decrease until 0), lest Backup cannot changes its status due to lower priority than the Master when the Master fails. After the interface monitored turns up over again, the priority of corresponding router (or L3 Ethernet switch) will restore in Backup.

Example: Configuring VRRPv3 monitor interface to VLAN 2 and decreasing amount of priority to 10.

```
Switch(Config-router)# circuit-failover vlan 2 10
```

55.3 debug ipv6 vrrp

Command: debug ipv6 vrrp [all | events | packet [recv | send]]

no debug ipv6 vrrp [all | events | packet [recv | send]]

Function: Display the state change, message receiving and sending of a VRRPv3 backup group, the no operation of this command will disable the display of DEBUG.

Parameters: None.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 vrrp
Jan 01 01:03:13 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:14 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:15 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]
```

55.4 disable

Command: disable

Function: Disable VRRPv3 virtual router.

Parameters: None.

Command Mode: VRRPv3 Protocol Mode.

Default: There is no configuration by default.

Usage Guide: Disable the corresponding virtual router session. Only after disabling the virtual router, can the relative configuration parameters be changed.

Examples: Disable the VRRPv3 virtual router whose ID is 10.

```
Switch(config)#router ipv6 vrrp 10
```

```
Switch(config-router)#disable
```

55.5 enable

Command: enable

Function: Enable VRRPv3 virtual router.

Parameters: None.

Command Mode: VRRPv3 Protocol Mode.

Default: There is no configuration by default.

Usage Guide: Start the corresponding virtual router session. Only the interface of the enabled router (or the layer-three switch) can actually join the backup group. Before enabling the virtual router, the virtual IPv6 address and interface of VRRPv3 should be configured.

Example: Enable the VRRPv3 virtual router whose ID is 10.

```
Switch(config)#router ipv6 vrrp 10
```

```
Switch(config-router)#enable
```

55.6 preempt-mode

Command: preempt-mode {true | false}

Function: Configure the preempt mode of VRRPv3.

Parameters: None.

Command Mode: VRRPv3 Protocol Mode.

Default: It is preempt mode by default.

Usage Guide: If it is needed that a router (or a layer-three switch) with higher priority can the role of master router, the preempt mode needs to be configured.

Example: Configure VRRPv3 as non-preempt mode.

```
Switch(config-router)# preempt-mode false
```

55.7 priority

Command: priority <*value*>

Function: Configure the priority of VRRPv3.

Parameters: <*value*> is the priority, whose range is from 1 to 254.

Command Mode: VRRPv3 Protocol Mode.

Default: Backup routers（or layer-three switches）all have a priority of 100, the priority of IP address owners are all 255 in the backup group they belong to.

Usage Guide: Priority decides the state of a router (or a layer-three Ethernet switch) in a backup group. The higher the priority is, the more possible the router can be a Master. The configurable priority ranges from 1 to 254, while the priority of 255 is reserved to the IP address owner. The priority of 0 has special usage, which is when disabling a VRRP session, Master will send an advertisement message with a priority of 0. When Backup receives such advertisement message, it will start a new round of Master selection. When there are two or more routers (or layer-three switches) in one backup group have the same priority, the router with biggest local link IPv6 address has higher priority.

Example: Configure the priority of VRRPv3 as 150.

```
Switch(config-router)# priority 150
```

55.8 router ipv6 vrrp

Command: router ipv6 vrrp <*vrid*>

no router ipv6 vrrp <*vrid*>

Function: Create or delete a VRRPv3 virtual router.

Parameters: <*vrid*> is the ID of the virtual router, the valid range is 1 to 255.

Command Mode: Global Mode.

Default: There is no configuration by default.

Usage Guide: This command is used to create or delete a VRRPv3 virtual router. The virtual router is uniquely specified by the virtual router ID and the related virtual IPv6 address. Only after creating a virtual router, relative configuration can be set on it. Considering the stability, the number of configurable virtual routers should not be more than 64.

Example: Configure a virtual router whose ID is10.

```
Switch(config)# router ipv6 vrrp 10
```

55.9 show ipv6 vrrp

Command: show ipv6 vrrp [<*vrid*>]

Function: Display the state and configuration information of VRRPv3 backup group.

Parameters: <*vrid*>is the ID of the virtual router, whose range is from 1 to 255, no parameter means to display the state and configuration infomation of all backup gorups.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show ipv6 vrrp
VrId 1
  State is Master
  Virtual IPv6 is fe80::2 (Not IPv6 owner)
  Interface is Vlan1
  Configured priority is 150, Current priority is 150
  Advertisement interval is 100 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 3, Status UP
VrId 10
  State is Initialize
  Virtual IPv6 is fe80::3 (Not IPv6 owner)
  Interface is Vlan2
  Priority is 100
  Advertisement interval is 300 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan2, Priority Delta 10, Status UP
```

Display Explanation
State State.
Virtual IPv6 Virtual IPv6 address.
Interface

Interface name.
Priority Priority.
Advertisement interval The interval of VRRPv3 advertisement messages.
Preempt Preempt mode.
Circuit failover interface Monitor interface information.

55.10 virtual-ipv6 interface

Command: virtual-ipv6 <*ipv6-address*> interface {Vlan <*ID*>| *IFNAM*E}

no virtual-ipv6 interface

Function: Configure the virtual IPv6 address and interface of VRRPv3.

Parameters: <*ipv6-address*>is the virtual IPv6 address, which has to be an IPv6 local link address.

{Vlan <*ID*>| *IFNAM*E} is the interface name.

Command Mode: VRRPv3 Protocol Mode.

Default: There is no configuration by default.

Usage Guide: This command is used to add an IPv6 address and interface to an existing backup group. The no operation of this command will delete the virtual IPv6 address and interface of the specified backup group. The virtual IPv6 address is the link local unicast address. There can only be one virtual IPv6 address in a backup group. In order to avoid the fault of returning physical MAC address when Ping virtual IPv6 address, it is regulated that the virtual IPv6 address should not be the real IPv6 address of the interface. Thus, the interfaces of all VRRPv3 backup groups are Backup by default, and need to select a Master within the backup groups.

Example: Configure the virtual IPv6 address of the backup group as fe80::2, the interface is VLAN1.

```
Switch(config-router)# virtual-ipv6 fe80::2 interface vlan 1
```

Chapter 56 Commands for MRPP

56.1 control-vlan

Command: control-vlan <*vid*>

no control-vlan

Function: Configure control VLAN ID of MRPP ring; the"**no control-vlan**" command deletes control VLAN ID.

Parameter: <*vid*> expresses control VLAN ID, the valid range is from 1 to 4094.

Command Mode: MRPP ring mode

Default: None

Usage Guide: The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094.To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may can't work normally or form broadcast.

The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function is enabled.

Example: Configure control VLAN of mrpp ring 4000 is 4000.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
```

56.2 clear mrpp statistics

Command: clear mrpp statistics [<*ring-id*>]

Function: Clear statistic information of MRPP data packet of MRPP ring receiving and transferring.

Parameter: <*ring-id*> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.

Command Mode: Admin Mode.

Default: None.

Usage Guide: None.

Example: Clear statistic information of MRPP ring 4000 of switch.

```
Switch#clear mrpp statistics 4000
```

56.3 debug mrpp

Command: debug mrpp

no debug mrpp

Function: Open MRPP debug information; "**no description**" command disables MRPP debug information.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable MRPP debug information, and check message process of MRPP protocol and receive data packet process, it is helpful to monitor debug.

Example: Enable debug information of MRPP protocol.

```
Switch#debug mrpp
```

56.4 enable

Command: enable

no enable

Function: Enable configured MRPP ring, the "**no enable**" command disables this enabled MRPP ring.

Parameter:

Command Mode: MRPP ring mode

Default: Default disable MRPP ring.

Usage Guide: Executing this command, it must enable MRPP protocol, and if other commands have configured, the MRPP ring is enabled.

Example: Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring.

```
Switch(config)#mrpp enable
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)# node-mode master
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(config)#in ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config)#in ethernet 1/3
Switch(config-If-Ethernet1/3)#mrpp ring 4000 secondary-port
```

56.5 fail-timer

Command: fail-timer <*timer*>

no fail-timer

Function: Configure if the primary node of MRPP ring receive Timer interval of Hello packet or not, the "**no fail-timer**" command restores default timer interval.

Parameter: <*timer*> valid range is from 1 to 300s.

Command Mode: MRPP ring mode

Default: Default configure timer interval 3s.

Usage Guide: If primary node of MRPP ring doesn't receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn't need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn't receive Hello packet on fail timer due to time delay.

Example: Configure fail timer of MRPP ring 4000 to 10s.

Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10

56.6 hello-timer

Command: hello-timer <*timer*>

no hello-timer

Function: Configure timer interval of Hello packet from primary node of MRPP ring, the"**no hello-timer**"command restores timer interval of default.

Parameter: <*timer*> valid range is from 1 to 100s.

Command Mode: MRPP ring mode

Default: Default configuration timer interval is 1s.

Usage Guide: The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.

Example: Configure hello-timer of MRPP ring 4000 to 3 seconds.

Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3

56.7 mrpp enable

Command: mrpp enable

no mrpp enable

Function: Enable MRPP protocol module, the "**no mrpp enable**" command disables MRPP protocol.

Parameter:

Command Mode: Global Mode

Default: The system doesn't enable MRPP protocol module.

Usage Guide: If it needs to configure MRPP ring, it enables MRPP protocol. Executing "**no mrpp enable**" command, it ensures to disable the switch enabled MRPP ring.

Example: Globally enable MRPP.

```
Switch(config)#mrpp enable
```

56.8 mrpp port-scan-mode

Command: mrpp port-scan-mode {interrupt | pool}

no mrpp port-scan-mode

Function: Set the scan mode of the mrpp port as "interrupt" or "pool".

Parameter: interrupt: the interrupt mode; pool: the pool mode.

Command Mode: Global Mode

Default: The default scan mode is active pool.

Example:

```
Switch(config)#mrpp enable
```

```
Switch(config)#mrpp port-scan-mode interrupt
```

56.9 mrpp ring

Command: mrpp ring *<ring-id>*

no mrpp ring *<ring-id>*

Function: Create MRPP ring, and access MRPP ring mode, the "**no mrpp ring*<ring-id>***" command deletes configured MRPP ring.

Parameter: *<ring-id>* is MRPP ring ID, the valid range is from 1 to 4096.

Command Mode: Global Mode

Usage Guide: If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "**no mrpp ring**" command.

```
Switch(config)#mrpp ring 100
```

56.10 mrpp ring primary-port

Command: mrpp ring *<ring-id>* primary-port

no mrpp ring *<ring-id>* primary-port

Function: Specify MRPP ring primary-port.

Parameter: *<ring-id>* is the ID of MRPP ring, range is <1-4096>.

Command Mode: Port mode

Default: None

Usage Guide: The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

The mrpp enable command must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.

Example: Configure the primary of MRPP ring 4000 to Ethernet 1/1.

Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

56.11 mrpp ring secondary-port

Command: mrpp ring < *ring-id* > secondary-port

no mrpp ring < *ring-id* > secondary-port

Function: Specify secondary of MRPP ring.

Parameter: <*ring-id*> is the ID of MRPP ring, range is <1-4096>.

Command Mode: Port mode

Default: None

Usage Guide: The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

The mrpp enable command must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.

Example: Configure secondary port of MRPP ring to 1/3.

Switch(config)#interface ethernet1/3
Switch(Config-If-Ethernet1/3)#mrpp ring 4000 secondary-port

56.12 node-mode

Command: node-mode {maser | transit}

Function: Configure the type of the node to primary node or secondary node.

Parameter:

Command Mode: MRPP ring mode

Default: Default the node mode is secondary node.

Usage Guide:

Example: Configure the switch to primary node. MRPP ring 4000.

Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master

56.13 show mrpp

Command: show mrpp [*ring-id*>]

Function: Display MRPP ring configuration.

Parameter: <*ring-id*> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.

Command Mode: Admin and Configuration Mode.

Default: None

Usage Guide: None

Example: Display configuration of MRPP ring 4000 of switch

```
Switch# show mrpp 4000
```

56.14 show mrpp statistics

Command: show mrpp statistics [<*ring-id*>]

Function: Display statistic information of data packet of MRPP ring receiving and transferring.

Parameter: <*ring-id*> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.

Command Mode: Admin and Configuration Mode.

Default: None

Usage Guide: None

Example: Display statistic information of MRPP ring 4000 of switch.

```
Switch# show mrpp statistic 4000
```

Chapter 57 Commands for ULPP

57.1 clear ulpp flush counter interface

Command: clear ulpp flush counter interface *<name>*

Function: Clear the statistic information of the flush packets.

Parameter: *<name>* is the name of the port.

Default: None.

Command mode: Admin mode.

Usage Guide: None.

Example: Clear the statistic information of the flush packets for the port1/1.

```
Switch# reset ulpp flush counter interface e1/1
ULPP flush counter has been reset.
```

57.2 control vlan

Command: control vlan *<integer>*

no control vlan

Function: Configure the control VLAN of ULPP group, the no command restores the default value.

Parameter: *<integer>* is the control VLAN ID that sends the flush packets, range from 1 to 4094.

Default: The default is VLAN 1.

Command mode: ULPP group configuration mode.

Usage Guide: Configure the control VLAN of ULPP group. Control vlan has no relation to the corresponding data VLAN that exist or don't exist, it is only used to match the receiving control VLAN.

Example: Configure the sending control VLAN of ULPP group as 10.

```
Switch(config)# ulpp group 20
```

```
Switch(ulpp-group-20)# control vlan 10
```

57.3 debug ulpp error

Command: debug ulpp error

no debug ulpp error

Function: Show the error information of ULPP. The no operation disables showing the error information of ULPP.

Parameter: None.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the error information of ULPP.

```
Switch# debug ulpp error
Unrecognized Flush packet received.
```

57.4 debug ulpp event

Command: debug ulpp event

no debug ulpp event

Function: Show the event information of ULPP. The no operation disables showing the event information of ULPP.

Parameter: None.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the event information of ULPP.

```
Switch# debug ulpp event
ULPP group 1 state changes：
Master port ethernet 1/1 in ULPP group 1 changed state to Forwading.
Slave port ethernet 1/2 in ULPP group 1 changed state to Standby.
```

57.5 debug ulpp flush content interface

Command: debug ulpp flush content interface <*name*>

no debug ulpp flush content interface <*name*>

Function: Show the contents of the receiving flush packets. The no operation disables the shown contents.

Parameter: <*name*> is the name of the port.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the contents of the receiving flush packets for the port1/1.

```
Switch# debug ulpp flush content interface e1/1
Flush packet content:
Destination MAC: 01-03-0f-cc-cc-cc
Source MAC: 00-a0-cc-d7-5c-ea
Type: 8100
Vlan ID: 1
Length: 518
Control Type: 2
Control Vlan: 10
MAC number:0
Vlan Bitmap:
```

57.6 debug ulpp flush {send | receive} interface

Command: debug ulpp flush {send | receive} interface <*name*>

no debug ulpp flush {send | receive} interface <*name*>

Function: Show the information of the receiving/sending flush packets, it only shows the receiving packets, but do not show the detailed contents of the packets. The no operation disables the shown information.

Parameter: <*name*> is the name of the port.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the information that send the flush packets for the port1/1.

```
Switch# debug ulpp flush send interface e1/1
Flush packet send on port Ethernet 1/1.
```

57.7 description

Command: description <*string*>

no description

Function: Configure the description character string of ULPP group. The no command deletes the description.

Parameter: <*string*> is the name of ULPP group, the max number of the characters is 128.

Default: Do not configure ULPP name by default.

Command mode: ULPP group configuration mode.

Usage Guide: None.

Example: Configure the description of ULPP group as PLANET.

```
Switch(config)# ulpp group 20
```

```
Switch(ulpp-group-20)# description PLANET
```

57.8 flush disable arp

Command: flush disable arp

Function: Disable sending the flush packets of deleting ARP.

Parameter: None.

Default: By default, enable the sending function of the flush packets which are deleted by ARP.

Command mode: ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.

Example: Disable sending the flush packets of deleting ARP.

```
Switch(config)# ulpp group 20
```

```
Switch(ulpp-group-20)# flush disable arp
```

57.9 flush disable mac

Command: flush disable mac

Function: Disable sending the flush packets of updating MAC address.

Parameter: None.

Default: By default, enable sending the flush packets of updating MAC address.

Command mode: ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.

Example: Disable sending the flush packets of updating MAC address.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable mac
```

57.10 flush enable arp

Command: flush enable arp

Function: Enable sending the flush packets of deleting ARP.

Parameter: None.

Default: By default, enable sending the flush packets of deleting ARP.

Command mode: ULPP group configuration mode.

Usage Guide: If enable this function, when the link is switched, it will actively send the flush packets to notify the upstream device, so as to delete the list entries of ARP.

Example: Enable sending the flush packets of deleting ARP.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable arp
```

57.11 flush enable mac

Command: flush enable mac

Function: Enable sending the flush packets of updating MAC address.

Parameter: None.

Default: By default, enable sending the flush packets of updating MAC address.

Command mode: ULPP group configuration mode.

Usage Guide: If enable this function, when the link is switched, it will actively send the flush packets to notify the upstream device, so as to update the MAC address table.

Example: Enable sending the flush packets of updating MAC address.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable mac
```

57.12 preemption delay

Command: preemption delay <*integer*>

no preemption delay

Function: Configure the preemption delay, the no command configures the preemption delay as the default value.

Parameter: <*integer*>: the preemption delay, range from 1 to 600, in second.

Default: The default preemption delay is 30.

Command mode: ULPP group configuration mode.

Usage Guide: The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.

Example: Configure the preemption delay as 50s for ULPP group.

Switch(config)# ulpp group 20
Switch(ulpp-group-20)# preemption delay 50

57.13 preemption mode

Command: preemption mode

no preemption mode

Function: Open/close the preemption mode of ULPP group.

Parameter: None.

Default: Do not preempt.

Command mode: ULPP group configuration mode.

Usage Guide: If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay,.

Example: Configure the preemption mode of ULPP group.

Switch(config)# ulpp group 20
Switch(ulpp-group-20)# preemption mode

57.14 protect vlan-reference-instance

Command: protect vlan-reference-instance <*instance-list*>

no protect vlan-reference-instance <*instance-list*>

Function: Configure the protective VLANs of ULPP group, the no command cancels the protective VLANs.

Parameter: <*instance-list*> is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.

Default: Do not protect any VLANs by default that means any instances are not quoted.

Command mode: ULPP group configuration mode.

Usage Guide: Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, multiple ULPP groups can quote the same instance.

Example: Configure the protective VLAN quoted from instance 1 for ULPP group.

```
Switch(config)# ulpp group 20
```

```
Switch(ulpp-group-20)# protect vlan-reference-instance 1
```

57.15 show ulpp flush counter interface

Command: show ulpp flush counter interface <*name*>

Function: Show the statistic information of the flush packets.

Parameter: <*name*> is the name of the ports.

Default: None.

Command mode: Admin mode.

Usage Guide: Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.

Example: Show the statistic information of the flush packets for ULPP group1.

```
Switch# show ulpp flush counter interface e1/1
Received flush packets: 10
```

57.16 show ulpp flush-receive-port

Command: show ulpp flush-receive-port

Function: Show the port which receive flush packet, flush type and control VLAN .

Parameter: None.

Default: None.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the information that the port receives flush packets.

```
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname            Type    Control Vlan
-------------------------------------------------
Ethernet1/1         ARP     1
Ethernet1/3         MAC     1;3;5-10
```

57.17 show ulpp group

Command: show ulpp group [group-id]

Function: Show the configuration information of the ULPP groups which have been configured.

Parameter: [group-id]: Show the information of the specific ULPP group.

Default: By default, show the information of all ULPP groups which have been configured.

Command mode: Admin mode.

Usage Guide: Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.

Example: Show the configuration information of ULPP group1.

```
Switch# show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member              Role          State
--------------------------------------------------------------
Ethernet1/1         MASTER        FORWARDING
Ethernet1/2         SLAVE         STANDBY
```

57.18 ulpp control vlan

Command: ulpp control vlan *<vlan-list>*

no ulpp control vlan *<vlan-list>*

Function: Configure the receiving control VLANs of the port, the no command restores the default value.

Parameter: *<vlan-list>* specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string can not exceed 100. The receiving control VLAN of the port can be added.

Default: The default is VLAN 1.

Command mode: Port mode.

Usage Guide: Configure the receiving control VLAN of the port. The control VLAN has no relation with the data VLAN whether exist or not, it is only used to match the sending control VLAN of the packets.

Example: Configure the receiving control VLAN as 10.

```
Switch(config)# interface ethernet 1/1
```

```
Switch(config-If-Ethernet1/1)# ulpp control vlan 10
```

57.19 ulpp flush disable arp

Command: ulpp flush disable arp

Function: Disable receiving the flush packets of deleting ARP.

Parameter: None.

Default: By default, disable receiving the flush packets of deleting ARP.

Command mode: Port mode.

Usage Guide: If this command is configured, then it will not receive the flush packets of deleting ARP.

Example: Disable receiving the flush packets of deleting ARP.

```
Switch(config)# interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp flush disable arp
```

57.20 ulpp flush disable mac

Command: ulpp flush disable mac

Function: Disable receiving the flush packets of updating MAC address.

Parameter: None.

Default: By default, disable receiving the flush packets of updating MAC address.

Command mode: Port mode.

Usage Guide: If this command is configured, then it will not receive the flush packets of updating MAC address.

Example: Disable receiving the flush packets of updating MAC address.

```
Switch(config)# interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp flush disable mac
```

57.21 ulpp flush enable arp

Command: ulpp flush enable arp

Function: Enable receiving the flush packets of deleting ARP.

Parameter: None.

Default: By default, disable receiving the flush packets of deleting ARP.

Command mode: Port mode.

Usage Guide: Enable this function to receive the flush packets which delete ARP.

Example: Enable receiving of the flush packets of deleting ARP.

```
Switch(config)# interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp flush enable arp
```

57.22 ulpp flush enable mac

Command: ulpp flush enable mac

Function: Enable receiving the flush packets of updating MAC address.

Parameter: None.

Default: By default, disable receiving the flush packets of updating MAC address.

Command mode: Port mode.

Usage Guide: Enable receiving the flush packets of updating MAC address table.

Example: Enable receiving the flush packets of updating the MAC address.

```
Switch(config)# interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp flush enable mac
```

57.23 ulpp group

Command: ulpp group *<integer>*

no ulpp group *<integer>*

Function: Create a ULPP group. If this group exists, then enter the configuration mode of ULPP group. The no command deletes a ULPP group.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Command mode: Global Mode.

Default: Any ULPP groups are not configured.

Usage Guide: None.

Example: Configure ulpp group 20 or enter the mode of ulpp group 20.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)#
```

57.24 ulpp group master

Command: ulpp group *<integer>* master

no ulpp group *<integer>* master

Function: Configure the master port of ULPP group, the no command deletes the master port.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Default: There is no master port configured by default.

Command mode: Port mode.

Usage Guide: There are no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.

Example: Configure the master port of ULPP group.

```
Switch(config)# interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp group 20 master
```

57.25 ulpp group slave

Command: ulpp group *<integer>* slave

no ulpp group *<integer>* slave

Function: Configure the slave port of ULPP group, the no command deletes the slave port.

Parameter: *<integer>* is the ID of ULPP group, the range from 1 to 48.

Default: There is no slave port configured by default.

Command mode: Port mode.

Usage Guide: There are no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one slave port, if the slave port exists, then the configuration is fail.

Example: Configure the slave port of ULPP group.

```
Switch(config)# interface ethernet 1/2
Switch(config-If-Ethernet1/2)# ulpp group 20 slave
```

Chapter 58 Commands for ULSM

58.1 debug ulsm event

Command: debug ulsm event

no debug ulsm event

Function: Show the event information of ULSM. The no operation disables showing ULSM events.

Parameter: None.

Default: None.

Command mode: Admin Mode.

Usage Guide: None.

Example: Show the event information of ULSM.

```
Switch# debug ulsm event
Downlink synchoronized with ULSM group, change state to Down.
```

58.2 show ulsm group

Command: show ulsm group [group-id]

Function: Show the configuration information of ULSM group.

Parameter: [group-id]: the ID of ULSM group.

Default: By default, show the information of all ULSM groups which have been configured.

Command mode: Admin Mode.

Usage Guide: None.

Example: Show the configuration information of ULSM group1.

```
Switch# show ulsm group 1
ULSM group 1 information:
ULSM group state: Up
Member          Role          State          Down by ULSM
-------------------------------------------------------------------------------
ethernet1/1     UpLINK        Up
ethernet1/2     DownLINK      Down           Yes
ethernet1/3     DownLINK      Up
```

58.3 ulsm group

Command: ulsm group *<group-id>*

no ulsm group *<group-id>*

Function: Create a ULSM group. The no command deletes the ULSM group.

Parameter: *<group-id>* is the ID of ULSM group, range from 1 to 32.

Default: There is no ULSM group configured by default.

Command mode: Global Mode.

Usage Guide: None.

Example: Create ULSM group 10.

```
Switch(config)# ulsm group 10
```

58.4 ulsm group {uplink | downlink}

Command: ulsm group <*group-id*> {uplink | downlink}

no ulsm group <*group-id*>

Function: Configure the uplink/downlink ports of ULSM group. The no command deletes the uplink/downlink ports.

Parameter: <*group-id*>: The ID of ULSM group, the range from 1 to 32.

uplink: Configure the port as the uplink port.

downlink: Configure the port as the downlink port.

Default: The port does not belong to any ULSM group.

Command mode: Port Mode.

Usage Guide: Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most.

Example: Configure port1/3 as the uplink port of ULSM group10.

```
Switch(config)# interface ethernet 1/3
```

```
Switch(config-If-Ethernet1/3)# ulsm group 10 uplink
```

Chapter 59 Commands for SNTP

59.1 debug sntp

Command: debug sntp {adjust | packet | select }

no debug sntp {adjust | packet | select}

Function: Displays or disables SNTP debug information.

Parameters: adjust stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection.

Command mode: Admin Mode

Example: Displaying debugging information for SNTP packet.

```
Switch#debug sntp packet
```

59.2 sntp server

Command: sntp server {<*server_address*> | <*server_ipv6_addr*>} [version <*version_no*>]

no sntp server { <*server_address*> | <*server_ipv6_addr*> }

Function: Configure the IPv4/IPv6 addresses and the version of the SNTP/NTP server; the “no” form of this command cancels the configured SNTP/NTP server addresses.

Parameter: ***<server_address>*** is the IPv4 unicast address of the SNTP/NTP server, ***<server_ipv6_addr>*** is the IPv6 unicast address of the SNTP/NTP server, ***<version_no>*** is the version No. of the SNTP on current server, ranging between 1-4 and defaulted at 1.

Default: No SNTP/NTP configured by default.

Command Mode: Global Mode

Example:

(1) Configure an IPv4 address of a SNTP/NTP server. SNTPv4 version is adopted on the **server**

```
Switch(config)#sntp server 10.1.1.1 version 4
```

(2) Configure a SNTP/NTP server IPv6 address

```
Switch(config)#sntp server 3ffe:506:1:2::5
```

59.3 sntp polltime

Command: sntp polltime <*interval*>

no sntp polltime

Function: Sets the interval for SNTP clients to send requests to NTP/SNTP; the “**no sntp polltime**” command cancels the polltime sets and restores the default setting.

Parameters: <*interval*> is the interval value from 16 to 16284.

Default: The default polltime is 64 seconds.

Command Mode: Global Mode

Example: Setting the client to send request to the server every 128 seconds.

```
Switch#config
Switch(config)#sntp polltime128
```

59.4 sntp timezone

Command: sntp timezone <*name*> [{add | subtract}] [<*time_difference*>]

no sntp timezone

Function: Set the difference between local time and UTC time. The no operation of this command cancels the configuration timezone and restores the default value.

Parameter: <*name*> is the name of local timezone, consist of max 16 characters. **<*add*>** means the timezone equals the UTC time add <time_difference>.**<*subtract*>**means the timezone equals the UTC time subtract <time_difference>.**<*time-difference*>** is the time difference to UTC time, range from 0 to 12,the default value is 8 .

Default: Add 8 is default timezone.

Command Mode: Global Mode

Example: Set the timezone Beijing.

```
Switch#config
Switch(config)#sntp timezone beijing add 8
```

59.5 show sntp

Command: show sntp

Function: Displays current SNTP client configuration and server status.

Parameters: N/A.

Command Mode: Admin and Configuration Mode.

Example: Displaying current SNTP configuration.

```
Switch#show sntp
SNTP server       Version      Last Receive
2.1.0.2             1              6
```

Chapter 60 Commands for NTP

60.1 ntp enable

Command: ntp enable

ntp disable

Function: To enable/disable NTP function globally.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP function.

```
Switch(config)#ntp enable
```

60.2 ntp server

Command: ntp server {<*ip-address*> | <*ipv6-address*>} [version <*version_no*>] [key <*key-id*>]

no ntp server {<*ip-address*>|<*ipv6-address*>}

Function: To enable specified time server of time source, the no form of this command cancels the specified time server of time source.

Parameter: ip-address: IPv4 address of time server.

ipv6-address: IPv6 address of time server.

version: The version information configured for server.

version_no: The version number of server, range is from 1 to 4, default is 4.

key: To configure key for server.

key-id: The key id.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure time server address as 1.1.1.1 on switch.

```
Switch(config)#ntp server 1.1.1.1
```

60.3 ntp broadcast server count

Command: ntp broadcast server count <*number*>

no ntp broadcast server count

Function: Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.

Parameters: number：1-100, the max number of broadcast servers.

Default: The default max number of broadcast servers is 50.

Command Mode: Global Mode.

Examples: Configure the max number of broadcast servers is 70 on the switch.

```
Switch(config)#ntp broadcast server count 70
```

60.4 ntp timezone

Command: ntp timezone <*name*> [{add | subtract}] [<*time_difference*>]

no ntp timezone

Function: To configure the time zone and time different with UTC for NTP client, the no form of this command cancels the time zone sets and restores the default setting.

Parameter: name is the configured time zone, less than 16 characters.

add means the configured UTC time add time_difference.

subtract means the configured UTC time subtract time_difference, add is by default.

time_difference is the configured time different , range between 0 to 12, set to 8 is by default.

Default: The time different is set to add 8 by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure the time zone to beijing.

```
Switch#config
```

```
Switch(config)#ntp timezone beijing add 8
```

60.5 ntp access-group

Command: ntp access-group server <*acl*>

no ntp access-group server <*acl*>

Function: To configure/cancel the access control list of NTP Server.

Parameter: <*acl*>: ACL number, range is from 1 to 99.

Default: Not configure the access control of NTP Server.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure access control list 2 on the switch.

```
Switch(config)#ntp access-group server 2
```

60.6 ntp authenticate

Command: ntp authenticate

no ntp authenticate

Function: To enable/cancel NTP authentication function.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP authentication function.

```
Switch(config)#ntp authenticate
```

60.7 ntp authentication-key

Command: ntp authentication-key <*key-id*> md5 <*value*>

no ntp authentication-key <*key-id*>

Function: To enable/cancel NTP authentication function, and defined NTP authentication key.

Parameter: key-id: The id of key, range is from 1 to 4294967295.

value: The value of key, range between 1 to 16 of ascii code.

Default: The authentication key of NTP authentication is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc.

```
Switch(config)# ntp authentication-key 20 md5 abc
```

60.8 ntp trusted-key

Command: ntp trusted-key <*key-id*>

no ntp trusted-key <*key-id*>

Function: To configure the trusted key. The no command cancels the trusted key.

Parameter: key-id: The id of key, range is from 1 to 4294967295.

Default: Trusted key is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure the specified key 20 to trusted key.

```
Switch(config)# ntp trusted-key 20
```

60.9 ntp disable

Command: ntp disable

no ntp disable

Function: To disable/enable the NTP function on port.

Parameter: None.

Default: To enable NTP function on all ports.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To disable the NTP function on vlan1 interface.

```
Switch(config)# interface vlan 1
```

```
Switch(Config-if-Vlan1)#ntp disable
```

60.10 ntp broadcast client

Command: ntp broadcast client

no ntp broadcast client

Function: To configure/cancel the specified port to receive NTP broadcast packets.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To enable the function of VLAN1 interface to receive NTP broadcast packets.

Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp broadcast client

60.11 ntp multicast client

Command: ntp multicast client

no ntp multicast client

Function: To configure/cancel the specified port to receive NTP multicast packets.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To enable the function of VLAN1 interface to receive NTP multicast packets.

Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp multicast client

60.12 ntp ipv6 multicast client

Command: ntp ipv6 multicast client

no ntp ipv6 multicast client

Function: To configure/cancel the specified port to receive NTP multicast packets of IPv6.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To enable the function of VLAN1 interface to receive NTP multicast packets of IPv6.

Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ntp ipv6 multicast client

60.13 debug ntp authentication

Command: debug ntp authentication

no debug ntp authentication

Function: To display NTP authentication information, the no form command disabled the switch of displaying NTP authentication information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: To display NTP authentication information, if the switch is enabled, and if the packets schlepped authentication information when the packet in sending or receiving process, then the key identifier will be printed out.

Example: To enable the switch of displaying NTP authentication information.

```
Switch# debug ntp authentication
```

60.14 debug ntp packet

Command: debug ntp packet [send | receive]

no debug ntp packet [send | receive]

Function: To enable/disable the debug switch of displaying NTP packet information.

Parameter: send: The debug switch of sending NTP packet.

receive: The debug switch of receiving NTP packet.

If there is no parameter, that means should enable the sending and receiving switch of NTP packet in the same time.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying NTP packet information.

```
Switch# debug ntp packet
```

60.15 debug ntp adjust

Command: debug ntp adjust

no debug ntp adjust

Function: To enable/disable the debug switch of displaying local time adjust information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying local time adjust information.

```
Switch# debug ntp adjust
```

60.16 debug ntp sync

Command: debug ntp sync

no debug ntp sync

Function: To enable/disable debug switch of displaying local time synchronization information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debug switch of displaying local time synchronization information.

```
Switch# debug ntp sync
```

60.17 debug ntp events

Command: debug ntp events

no debug ntp events

Function: To enable/disable debug switch of displaying NTP event.

Parameter: None.

Default: Disable the debug switch of displaying NTP event.

Command Mode: Admin Mode.

Usage Guide: To enable debug switch of displaying NTP event, after that, if some server changed from available to unavailable or from unavailable to available, the received illegal packet events will be printed.

Example: To enable debug switch of displaying NTP event information.

```
Switch# debug ntp events
```

60.18 show ntp status

Command: show ntp status

Function: To display time synchronization status, include synchronized or not, layers, address of time source and so on.

Parameter: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: None.

Example:

```
Switch# show ntp status
Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006
```

60.19 show ntp session

Command: show ntp session [<*ip-address*> | <*ipv6-address*>]

Function: To display the information of all NTP session or some one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)

Parameter: ip-address: The IPv4 address of some specifics configured time server.

ipv6-address: The IPv6 address of some specifics configured time server.

If no parameter, the session relative information of all servers will be displayed (Include broadcast and multicast servers)

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: None.

Example:

```
Switch# show ntp session
    server          stream      type      rootdelay      rootdispersion      trustlevel
*   1.1.1.2           2         unicast     0.010s           0.002s             10
    2.2.2.2           3         unicast     0.005s           0.000s             10
```

Chapter 61 Commands for DNSv4/v6

61.1 clear dynamic-host

Command: clear dynamic-host {<*ip-address*> | <*ipv6-address*> | all}

Function: To delete the domain entry of specified address or all address in dynamic cache.

Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation; ***<ipv6-address>*** is the IPv6 address; **all** is to delete the domain entry of all address in dynamic cache.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: This command is used to manually delete the domain name and address entry in dynamic cache, this command is much useful when domain name have lived long time in cache.

Example: To delete the address of 202.108.22.5 of domain entry.

```
Switch(config)# clear dynamic-host 202.108.22.5
```

61.2 debug dns

Command: debug dns {all | packet [send | recv] | events | relay}

no debug dns {all | packet [send | recv] | events | relay}

Function: To display the application debug information of DNS domain name resolution, the no form of this command disables the debug display.

Parameter: None.

Command Mode: Admin Mode.

Example:

```
Switch# debug dns all
```

```
Switch# ping host www.sina.com.cn

%Jan 01 00:03:13 2006 domain name www.sina.com.cn is to be parsed!
%Jan 01 00:03:13 2006 Dns query type is A!
  %Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 ......
ping www.sina.com.cn [202.108.33.32]
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 202.108.33.32, timeout is 2 seconds.
%Jan 01 00:03:15 2006 Host:www.sina.com.cn       Address:202.108.33.32
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms
```

61.3 dns-server

Command: dns-server {<*ip-address*>|<*ipv6-address*>} [priority <*value*>]

no dns-server {<*ip-address*>|<*ipv6-address*>}

Function: To configure/delete DNS server.

Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation, ***<ipv6-address>*** is the IPv6 address, ***<value>*** is the priority of DNS server, range between 0~255, 0 by default.

Command Mode: Global Mode.

Default: Not configuration.

Usage Guide: This command is used for configure or delete DNS server, when need to enable dynamic domain name mapping, the switch will sending a domain name search request packet to configured DNS server, the DNS server can be configured no more than 6. The priority is the optional parameter, if priority is configured, the DNS server must be organized according to the order of priority, from high to low. That is the switch sending domain name search request to the server which have the biggest priority, so some DNS server with quick search speed and used frequently can be configured to highest priority. If priority is not configured, to search DNS server must according to the configuration order. When the switch serves as a DNS SERVER, the queries to the DNS SERVER won't follow the above privilege rule; instead, the requests will be sent to all configured servers at the same time

Example: To configure the priority of DNS server as 200, the server's address is 10.1.120.241.

```
Switch(config)# dns-server 10.1.120.241 priority 200
```

61.4 dns lookup

Command: dns lookup {ipv4 | ipv6} <*hostname*>

Function: To enable DNS dynamic domain name resolution.

Parameter: {ipv4 | ipv6} means the IPv4 or IPv6 address look up, ***<hostname>*** is the resolute dynamic host name, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to look up correspond address based on entered client name, it can look up both IPv4 and IPv6 address. This command only used for domain name mapping, it have no other application function. When command is running, interrupt is forbidding. If configured many servers and domain name suffix, longer time will be required for domain name mapping.

Example: To look up the IPv4 address of www.sina.com.

```
Switch(config)# dns lookup ipv4 www.sina.com
```

61.5 show dns name-server

Command: show dns name-server

Function: To display the information of configured DNS server.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show dns name-server
DNS NAME SERVER:
Address                         Priority
10.1.120.231                    100
10.1.180.85                     80
```

```
2001::1                                    20
```

61.6 show dns domain-list

Command: show dns domain-list

Function: To display the suffix information of configured DNS domain name.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show dns domain-list
DNS DOMAIN LIST:
com.cn
edu.cn
```

61.7 show dns hosts

Command: show dns dynamic-hosts

Function: To display the dynamic domain name information of resolute by switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch# show dns dynamic-hosts
Total number of dynamic host is 2
DNS HOST LIST：
Hostname              Address                Time to live      Type
www.sina.com.cn       202.108.33.32              168000          dynamic
www.ipv6.org          2001:6b0:1:            168060          dynamic
```

61.8 show dns config

Command: show dns config

Function: Display the configured global DNS information on the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch(config)#show dns config
ip dns server enable
ip domain-lookup enable
the maximum of dns client in cache is 3000, timeout is 5
dns client number in cache is 0
dns dynamic host in cache is 0
dns name server number is 1
dns domain-list number is 0
```

61.9 show dns client

Command: show dns client

Function: Display the DNS Client information maintained by the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

```
Switch(config)#show dns client
DNS REQUEST LIST:
Total number of dns request is 2
Address                                  Request Id
192.168.11.141                           1
192.168.11.138                           2
```

61.10 ip domain-lookup

Command: ip domain-lookup

no ip domain-lookup

Function: To enable/disable DNS function, whether the switch will send dynamic DNS domain queries to the real DNS server or not.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to enable or disable the switch DNS dynamic query function. If DNS dynamic query function is enabled, the DNS server will resolve the host name and domain name to the IPv4 or IPv6 address for requests from the clients. If DNS is disabled, client applications will not be able to send any DNS requests to the DNS server. In this situation, only the static address resolution is available. For the address mapping in the resolve cache, which is learnt through DNS before, will be invalid after aging.

Example: To enable DNS function, can resolve the domain name dynamic.

```
Switch(config)# ip domain-lookup
```

61.11 ip domain-list

Command: ip domain-list *<WORD>*

no ip domain-list *<WORD>*

Function: To configure/delete domain name suffix.

Parameter: *<WORD>* is the character string of domain name suffix, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to configure or delete suffix of domain name, when the entered domain name is not integrity (such as sina), the switch can add suffix automatically, after that, address mapping can run, the domain name suffix can be configured no more than 6. The first configured domain name suffix will be added first.

Example: To configure domain name suffix of com.

```
Switch(config)# ip domain-list com
```

61.12 ip dns server

Command: ip dns server

no ip dns server

Function: Enable/disable DNS SERVER function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled by default.

Usage Guide: After the DNS SERVER function is enabled, the switch will be able to receive and handle DNS Requests from the clients by looking up locally or forward the request to the real DNS server.

Example: Configure to enable the dns server function of the switch.

```
Switch(config)#ip dns server
```

61.13 ip dns server queue maximum

Command: ip dns server queue maximum <1-5000>

no ip dns server queue maximum

Function: Configure the max number of client information in the switch queue.

Parameter: <1-5000> the value can be 1－5000.

Command Mode: Global Mode.

Default: The default client number is 3000.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the number of client information in the queue should not exceed the configured maximum number; otherwise the client's request won't be handled.

Example: Set the max number of client information in the switch queue as 2000.

```
Switch(config)#ip dns server queue maximum 2000
```

61.14 ip dns server queue timeout

Command: ip dns server queue timeout <1-100>

no ip dns server queue timeout

Function: Configure the timeout value of caching the client information on the switch.

Parameters: <1-100> the value can be1－100s.

Command Mode: Global Mode.

Default: The default timeout value is 5s.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the time of maintaining the client information should not exceed the configured maximum timeout value; otherwise the client's information will be cleared out.

Example: Configure the maximum timeout value of caching the client information on the switch as 10s.

```
Switch(config)#ip dns server queue timeout 10
```

Chapter 62 Commands for Show

62.1 clear logging

Command: clear logging {sdram | nvram}

Function: This command is used to clear all the information in the log buffer zone.

Command Mode: Admin Mode

Usage Guide: When the old information in the log buffer zone is no longer concerned, we can use this command to clear all the information.

Example: Clear all information in the log buffer zone sdram.

```
Switch#clear logging sdram
```

Related Command: show logging buffered

62.2 logging

Command: logging {<*ipv4-addr*> | <ipv6-addr>} [facility <*local-number*>] [level <*severity*>]

no logging {<*ipv4-addr*> | <ipv6-addr>}[facility <*local-number*>]

Function: The command is used to configure the output channel of the log host. The “no” form of this command will disable the output at the log host output channel.

Parameter: <*ipv4-addr*> is the IPv4 address of the host, **<ipv6-addr>** is the IPv6 address of the host; **<*local-number*>** is the recording equipment of the host with a valid range of local0～local7,which is in accordance with the facility defined in the RFC3164; **<*severity*>** is the severity threshold of the log information severity level, The rule of the log information output is explained as follows：only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.

Command Mode: Global Mode

Default: No log information output to the log host by default. The default recorder of the log host is the local0, the default severity level is warnings.

Usage Guide: Only when the log host is configured by the logging command, this command will be available. We can configure many IPv4 and IPv6 log hosts.

Example 1: Send the log information with a severity level equal to or higher than warning to the log server with an IPv4 address of 100.100.100.5, and save to the log recording equipment local1.

```
Switch(config)# logging 100.100.100.5 facility local1 level warnings
```

Example 2: Send the log information with a severity level equal to or higher than informational to the log server with an IPv6 address of 3ffe:506:1:2::3, and save to the log recording equipment local5.

```
Switch(config)# logging 3ffe:506:1:2::3 facility local1 level informational
```

62.3 ping

Command: ping [[src <*source-address*>] {<*destination-address*> | host <*hostname*> }]

Function: Issue ICMP request to remote devices, Check whether the remote device can be reached by the switch.

Parameters: <*source-address*> is the source IP address where the ping command is issued, with IP address in dotted decimal format. **<*destination-address*>** is the target IP address of the ping command, with IP address in dotted decimal format. **<*hostname*>** is the target host name of the ping command, which is limited to be less than 30 characters.

Default: 5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.

Command Mode: Admin mode

Usage Guide: When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.

Example:

Example 1: To ping with default parameters.

```
Switch#ping 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms
```

In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2: Use ping command with source address configuration, and leave other fields to default.

```
Switch#ping src 10.1.128.161 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is
2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

In the example above, 10.1.128.161 is configured as the source address of the ICMP echo requests, while the destination device is configured to be at 10.1.128.160. The command receives all the ICMP reply packets for all of the five ICMP echo requests. The success rate is 100%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 3: Ping with parameters entered interactively.

```
Switch#ping
VRF name：
Target IP address：10.1.128.160
```

```
Use source address option[n]: y
Source IP address: 10.1.128.161
Repeat count [5]：100
Datagram size in byte [56]：1000
Timeout in milli-seconds [2000]：500
Extended commands [n]：n
```

Display Information Explanation
VRF name VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address： The IP address of the target device.
Use source address option[n] Whether or not to use ping with source address.
Source IP address To specify the source IP address for ping.
Repeat count [5] Number of ping requests to be sent. the default value is 5.
Datagram size in byte [56] The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]： Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]： Whether or to use other extended options.

62.4 ping6

Command: ping6 [<*dst-ipv6-address*> | host <*hostname*> | src <*src-ipv6-address*> {<*dst-ipv6-address* > | *host* <*hostname*>}]

Function: To check whether the destination network can be reached.

Parameters: <*dst-ipv6-address*> is the target IPv6 address of the ping command. **<*src-ipv6-address*>** is the source IPv6 address where the ping command is issued. **<*hostname*>** is the target host name of the ping command, which is limited to be less than 30 characters.

Default: Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default timeout to be 2 seconds.

Command Mode: Normal user mode

Usage Guide: When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.

Example:

(1) To issue ping6 command with default parameters.

```
Switch>ping6 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms
```

(2) To issue the ping6 command with source IPv6 address specified.

```
switch>ping6 src 2001:1:2::3 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(3) To issue the ping6 command with parameters input interactively.

```
switch>ping6
Target IPv6 address:fe80::2d0:59ff:feb8:3b27
Output Interface: vlan1
Use source address option[n]:y
Source IPv6 address: fe80::203:fff:fe0b:16e3
Repeat count [5]:
Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
```

```
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

Display Information Explanation
ping6 The ping6 command
Target IPv6 address The target IPv6 address of the command.
Output Interface The name of he VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]: Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address Source IPv6 address.
Repeat count[5] Number of the ping packets.
Datagram size in byte[56] Packet size of the ping command. 56 byte by default.
Timeout in milli-seconds[2000] Timeout for ping command. 2 seconds by default.

Extended commands[n] Extended configuration. Disabled by default.
! The network is reachable.
. The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms Statistic information, success rate is 100 percent of ping packet.

62.5 show debugging

Command: show debugging {bgp | dvmrp | igmp | ipv6 | mld | nsm | ospf | other | pim | rip | spanning-tree | vrrp}

Function: Display the debug switch status.

Usage Guide: If the user needs to check what debug switches have been enabled, **show debugging** command can be executed.

Command mode: Admin Mode

Example: Check for currently enabled debug switch.

Switch#show debugging ospf OSPF debugging status: OSPF all IFSM debugging is on OSPF packet Hello detail debugging is on OSPF packet Database Description detail debugging is on OSPF packet Link State Request detail debugging is on OSPF packet Link State Update detail debugging is on OSPF packet Link State Acknowledgment detail debugging is on OSPF all LSA debugging is on OSPF all NSM debugging is on OSPF all events debugging is on OSPF all route calculation debugging is on
Switch#

Relative command: debug

62.6 show flash

Command: show flash

Function: Show the size of the files which are reserved in the system flash memory.

Command Mode: Admin Mode and Configuration Mode.

Example: To list the files and their size in the flash.

```
Switch#show flash
boot.rom                          329,828 1900-01-01 00:00:00 --SH
boot.conf                              94 1900-01-01 00:00:00 --SH
nos.img                         2,449,496 1980-01-01 00:01:06 ----
startup-config                      2,064 1980-01-01 00:30:12 ----
```

62.7 show history

Command: show history

Function: Display the recent user command history.

Command mode: Admin Mode

Usage Guide: The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

```
Switch#show history
enable
config
interface ethernet 1/3
enable
dir
show ftp
```

62.8 show logging buffered

Command: show logging buffered [level {*critical* | *warnings*} | range <*begin-index*> <*end-index*>]

Function: This command displays the detailed information in the log buffer channel. This command is not supported on low end switches.

Parameter: level {*critical* | *warnings*} means the level of critical information. **<*begin-index*>** is the index start value of the log message, the valid range is 1-65535, **<*end-index*>** is the index end value of the log message, the valid range is 1-65535. When only display logging buffered information of the line card must be added range parameter, but the main control has not the request.

Command Mode: Admin and Configuration Mode.

Default: No parameter specified indicates all the critical log information will be displayed.

Usage Guide: Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time <level> module ID [mission name] log information.

Example 1: Display the critical log information in the log buffer zone channel and related to the main control with index ID between 940 and 946.

```
Switch#show logging buffered level critical range 940 946
```

Example 2: Display all the information which level is warning in the log buffer zone channel.

```
Switch#show logging buffered level warning
```

62.9 show memory

Command: show memory [usage]

Function: Display the contents in the memory.

Parameter: usage means memory use information.

Command mode: Admin Mode

Usage Guide: This command is used for switch debug purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts: address, Hex view of the information and character view.

Example:

```
Switch#show memory
start address : 0x2100
number of words[64]:

002100:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002110:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002120:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002130:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002140:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002150:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002160:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
002170:   0000 0000 0000 0000   0000 0000 0000 0000   *................*
```

62.10 show running-config

Command: show running-config

Function: Display the current active configuration parameters for the switch.

Default: If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters.

Example:

```
Switch#show running-config
```

62.11 show startup-config

Command: show startup-config

Function: Display the switch parameter configurations written into the Flash memory at the current operation; those are usually also the configuration files used for the next power-up.

Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

62.12 show switchport interface

Command: show switchport interface [ethernet *<IFNAME>*]

Function: Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

Parameter: *<IFNAME>* is the port number.

Command mode: Admin mode

Example: Show VLAN messages of port ethernet 1/1.

```
Switch#show switchport interface ethernet 1/1
Ethernet1/1
Type :Universal
Mac addr num : No limit
Mode :Access
Port VID :1
Trunk allowed Vlan :ALL
```

Displayed Information Description
Ethernet1/1 Corresponding interface number of the Ethernet.
Type Current interface type.
Mac addr num Number of interfaces with MAC address learning ability.

Mode :Access Current interface VLAN mode.
Port VID :1 Current VLAN number the interface belongs.
Trunk allowed Vlan :ALL VLAN permitted by Trunk.

62.13 show tcp

Command: show tcp

Function: Display the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

```
Switch#show tcp
LocalAddress     LocalPort  ForeignAddress   ForeignPort      State
0.0.0.0          23         0.0.0.0          0                LISTEN
0.0.0.0          80         0.0.0.0          0                LISTEN
```

Displayed information Description
LocalAddress Local address of the TCP connection.
LocalPort Local pot number of the TCP connection.
ForeignAddress Remote address of the TCP connection.
ForeignPort Remote port number of the TCP connection.
State Current status of the TCP connection.

62.14 show telnet login

Command: show telnet login

Function: List information of currently available telnet clients which are connected to the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: This command used to list the information of currently available telnet clients which are connected to the switch.

Example:

```
Switch#show telnet login
Authenticate login by local.
Login user:
Aa
```

62.15 show temperature

Command: show temperature

Function: Show the temperature of the CPU.

Parameters: None.

Command Mode: Any modes

Usage Guide: This command can be used to monitor the CPU temperature of the switch.

Example: Show the temperature of the CPU of the switch.

```
Switch(Config)#show temperature
Temperature: 47.0625 ℃
```

62.16 show tech-support

Command: show tech-support

Function: Display various information about the switch and the running tasks. This command is used to diagnose the switch by the technical support specialist.

Command Mode: Admin mode and configuration mode

Usage Guide: When failure occurred on the switch, this command can be used to get related information, in order to diagnose the problems.

Example:

```
Switch#show tech-support
```

62.17 show udp

Command: show udp

Function: Display the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

```
Switch#show udp
LocalAddress      LocalPort   ForeignAddress    ForeignPort      State
0.0.0.0           161         0.0.0.0           0                CLOSED
0.0.0.0           123         0.0.0.0           0                CLOSED
0.0.0.0           1985        0.0.0.0           0                CLOSED
```

Displayed information Description
LocalAddress Local address of the UDP connection.
LocalPort Local pot number of the UDP connection.
ForeignAddress Remote address of the UDP connection.
ForeignPort Remote port number of the UDP connection.
State Current status of the UDP connection.

62.18 show version

Command: show version

Function: Display the switch version.

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version.

Example:

```
Switch#show version
```

62.19 traceroute

Command: traceroute [source <*ipv4-addr*>] { <*ip-addr*> | host <*hostname*> } [hops <*hops*>] [timeout <*timeout*>]

Function: This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Parameter: <*ipv4-addr*> is the assigned source host IPv4 address in dot decimal format. **<*ip-addr*>** is the target host IP address in dot decimal format. **<*hostname*>** is the hostname for the remote host. **<*hops*>** is the maximum gateway number allowed by Traceroute command. **<*timeout*>** Is the timeout value for test packets in milliseconds, between 100 -10000.

Default: The default maximum gateway number is 30, timeout in 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

62.20 traceroute6

Command: traceroute6 [source <*addr*>] {<*ipv6-addr*> | host <*hostname*>} [hops <*hops*>] [timeout <*timeout*>]

Function: This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.

Parameter: <*addr*> is the assigned source host IPv6 address in colonned hex notation. **<*ipv6-addr*>** is the IPv6 address of the destination host, shown in colonned hex notation;**<*hostname*>** is the name of the remote host; **<*hops*>** is the max number of the gateways the traceroute6 passed through, ranging between 1-255; **<*timeout*>** is the timeout period of the data packets, shown in millisecond and ranging between 100~10000.

Default: Default number of the gateways pass by the data packets is 30, and timeout period is defaulted at 2000 ms.

Command Mode: Admin Mode

Usage Guide: Traceroute6 is normally used to locate destination network inaccessible failures.

Example:

```
Switch# traceroute6 2004:1:2:3::4
```

Relevant Command: ipv6 host

Chapter 63 Commands for Reload Switch after Specified Time

63.1 reload after

Command: reload after <*HH:MM:SS*>

Function: Reload the switch after a specified period of time.

Parameters: <*HH:MM:SS*> the specified time period, HH（hours）ranges from 0 to 23, MM（minutes）and SS（seconds）range from 0 to 59.

Command Mode: Admin mode

Usage Guide: With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect.

Example: Set the switch to automatically reload in 10 hours and 1second.

```
Switch#reload after 10:00:01
Process with reboot after? [Y/N] y
```

Related Commands: reload, reload cancel, show reload

63.2 reload cancel

Command: reload cancel

Function: Cancel the specified time period to reload the switch.

Parameters: None

Command Mode: Admin mode.

Usage Guide: With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command ”reload after”. This command will not be reserved.

Example: Prevent the switch to automatically reboot after the specified time.

```
Switch#reload cancel
Reload cancel successful.
```

Related Commands: reload, reload after, show reload

63.3 show reload

Command: show reload

Function: Display the user’s configuration of command “reload after”.

Parameters: None.

Command Mode: Admin and configuration mode

Usage Guide: With this command, users can view the configuration of command “reload after” and check how long a time is left before rebooting the switch.

Example: View the configuration of command “reload after”. In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.

```
Switch#show reload
  The original reload after configuration is 10:00:01.
  System will be rebooted after 09:59:48 from now.
```

Related Commands: reload, reload after, reload cancel

Chapter 64 Commands for Debugging and Diagnosis for Packets Received and Sent by CPU

64.1 cpu-rx-ratelimit total

Command: cpu-rx-ratelimit total <packets>

no cpu-rx-ratelimit total

Function: Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default.

Parameter: <packets> is the max number of CPU receiving packets per second.

Command Mode: Global Mode

Default: 1200pps.

Usage Guide: The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the total rate of the CPU receive packets to 1500pps.

```
Switch(config)#cpu-rx-ratelimit total 1500
```

64.2 cpu-rx-ratelimit queue-length

Command: cpu-rx-ratelimit queue-length <queue-id> <qlen-value>

no cpu-rx-ratelimit queue-length <queue-id>

Function: Set the length of the specified queue, the no command set the length to default.

Parameter: <queue-id> is the index of specified queue, the range of the queue-id is <0-7>. <qlen-value> is the queue's length, the range of length is <0-500>pkts, 0 indicates closing the queue.

Command Mode: Global Mode

Default: Default length is 100pkts.

Usage Guide: The queue length set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the length of queue 2 to 150pkts.

```
Switch(config)#cpu-rx-ratelimit queue-length 2 150
```

64.3 cpu-rx-ratelimit protocol

Command: cpu-rx-ratelimit protocol *<protocol-type>* *<packets>*

no cpu-rx-ratelimit protocol *<protocol-type>*

Function: Set the max rate of the CPU receiving packets of the protocol type, the "**no cpu-rx-ratelimit protocol *<protocol-type>***" command set the max rate to default.

Parameter: ***<protocol-type>*** is the type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknown-mcast, unknow-mcast6, mld. ***<packets>*** is the max rate of CPU receiving packets of the protocol type, its range is 1-2000 pps.

Command Mode: Global Mode

Default: A different default rate is set for the different type of protocol.

Usage Guide: The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the rate of the CPU receiving the arp packets to 500pps.

```
Switch(config)#cpu-rx-ratelimit protocol arp 500
```

64.4 clear cpu-rx-stat protocol

Command: clear cpu-rx-stat protocol [<*protocol-type*>]

Function: Clear the statistics of the CPU received packets of the protocol type.

Parameter: <*protocol-type*> is the type of the protocol of the packet, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknown-mcast, unknow-mcast6, mld.

Command Mode: Global Mode

Usage Guide: This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.

Example: Clear the statistics of the CPU receives arp packets.

```
Switch(config)#clear cpu-rx-stat protocol arp
```

64.5 cpu-rx-ratelimit channel

This type of switch does not support the command.

64.6 show cpu-rx protocol

Command: show cpu-rx protocol [<*protocol-type*>]

Function: Show the statistics of the CPU received packets of the protocol type.

Parameter: <*protocol- type*> is the type of the protocol of the packet.

Command Mode: Admin Mode

Default: None.

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example：Show the statistics of the CPU receiving arp packets.

```
Switch#show cpu-rx protocol arp
Type                Rate-limit      TotPkts         CurState
arp                 500             3               allowed
```

64.7 debug driver

Command: debug driver {receive | send} [interface {<*interface-name*> | all}] [protocol {<*protocol-type*> | discard | all}] [detail]

no debug driver {receive | send}

Function: Turn on the on-off of showing the information of the CPU receiving or sending packets, the "**no debug driver {receive | send}**" command turn off the on-off.

Parameter: receive | send show the information of receiving or sending packets;

interface {<*interface-list*>| all}: interface-list is the Ethernet port number, **all** indicate all the Ethernet ports.

protocol {<*protocol-type*> | discard | all}: protocol-type is the type of the protocol of the packet, including snmp、telnet、http、dhcp、igmp、hsrp、arp、bgp、rip、ospf、pim、ssh、vrrp、ripng、ospfv3、pimv6、icmpv6、bgp4plus、unknown-mcast、unknown-mcast6、ttl0-2cpu、isis、dot1x、gvrp、stp、lacp、cluster、mld、vrrpv3、ra、uldp、lldp、eapou, **all** means all of the protocol types, **discard** means all the discarded packets.

Detail show detail information.

Command Mode: Admin Mode

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example: Turn on the on-off for showing the receiving packets.

```
Switch#debug driver receive
```