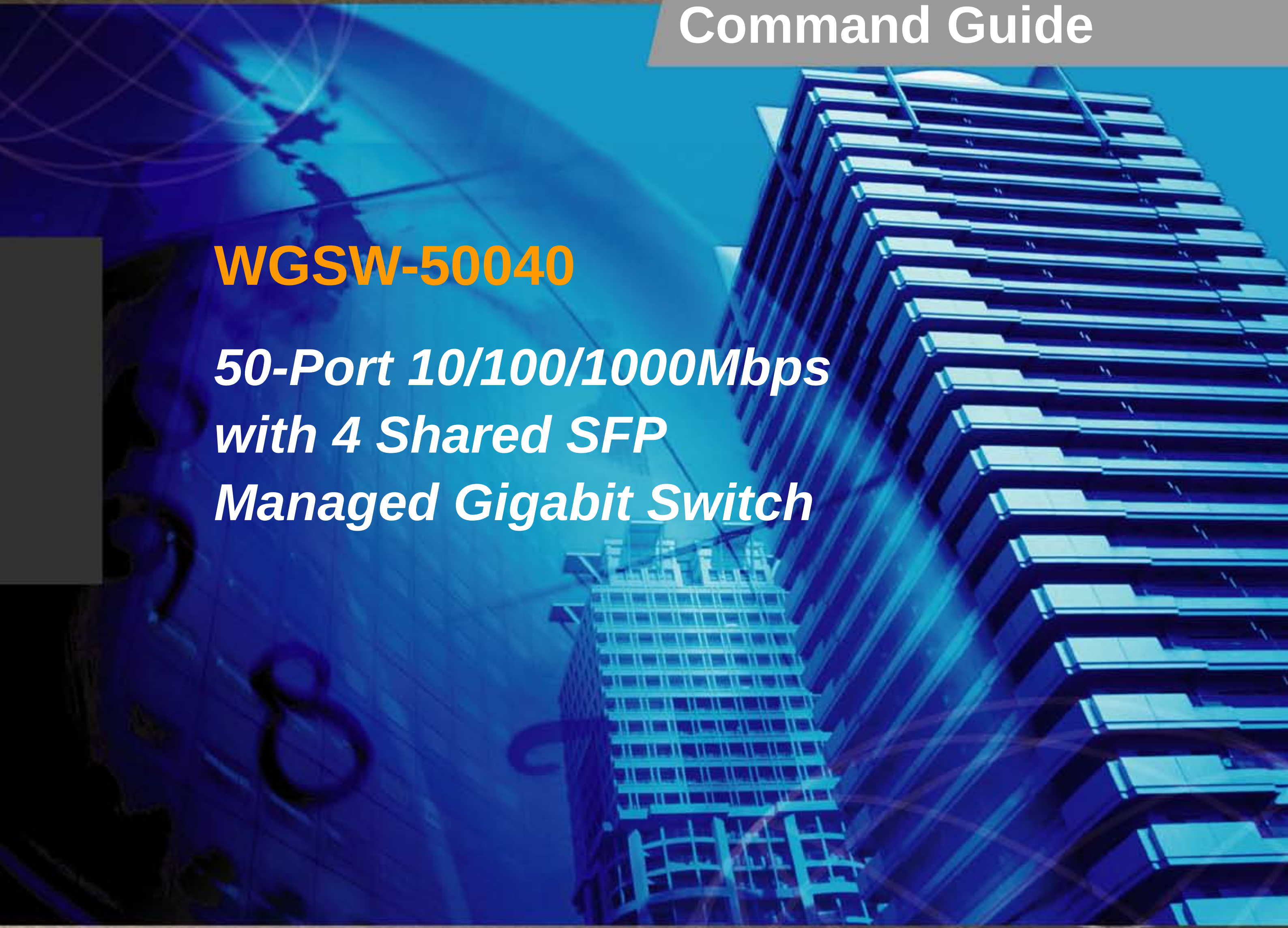
Command Guide



WGSW-50040

50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch

Content

Chapter 1 Commands for Basic Switch Configuration

1.1 Commands for Basic Configuration

1.1.1 Authentication line

Command:

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

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 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 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
```

1.1.3 config

Command:

config [terminal]

Function:

Enter Global Mode from Admin Mode.

Parameter:

[terminal] indicates terminal configuration.

Command mode:

Admin Mode.

Example:

```
Switch#config
```

1.1.4 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
```

1.1.5 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#
```

1.1.6 enable password

Command:

enable password [0|7] <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 password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

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 0 admin
```

1.1.7 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
```

1.1.8 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#
```

1.1.9 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#
```

1.1.10 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?'.)

1.1.11 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)#
```

1.1.12 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

1.1.13 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

1.1.14 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
```

1.1.15 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.

1.1.16 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
```

1.1.17 password

Command:

password [0|7] <*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 0 test
Switch(config)#login
```

1.1.18 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.

1.1.19 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
```

1.1.20 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
```

1.1.21 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
```

1.1.22 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
```

1.1.23 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
```

1.1.24 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.

1.1.25 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

1.1.26 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 ℃
```

1.1.27 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
```

1.1.28 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.
```

1.1.29 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
```

1.1.30 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.

1.1.31 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.

Paramters:

<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 authentication

Command:

authorization line {console | vty | web} exec {local | radius | tacacs}

no authorization line {console | vty | web} exec

Function:

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

Default:

There is no authorization mode.

Command Mode:

Global Mode.

Usage Guide:

The authorization method for Console, VTY and Web login can be configured respectively. And authorization 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 authorization method, authorization 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 authorization method; it will attempt the next authorization 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 local users adopt username command permission while authorization command is not configured, the users login the switch via RADIUS/TACACS method and works under common mode.

Example:

Configure the telnet authentication mode to RADIUS.

```
Switch(config)# authorization line vty exec radius
```

1.2.7 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
```

1.2.8 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
```

1.2.9 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:***
WGSW-50040>
```

1.2.10 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
```

1.2.11 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
```

1.2.12 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
```

1.2.13 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
```

1.2.14 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
```

1.2.15 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
```

1.2.16 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
```

1.2.17 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 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 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

1.3.3 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
```

1.3.4 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

1.3.5 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 [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 Commands for Cluster

2.1 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
```

2.2 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
```

2.3 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
```

2.4 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
```

2.5 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
```

2.6 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
```

2.7 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
```

2.8 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
```

2.9 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
```

2.10 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
```

2.11 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
```

2.12 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
```

2.13 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
```

2.14 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.

```
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
```

2.15 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      WGSW-50040         10.254.254.2
   2 A Active        00-01-02-03-04-05 MIS_bison       WGSW-50040         10.254.254.3
   3 U Active        00-01-02-03-04-05 SRD_jaguar     WGSW-50040         10.254.254.4
   4 A Inactive     00-01-02-03-04-05 HRD_puma      WGSW-50040         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: WGSW-50040
Hostname:   102
```

2.16 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 WGSW-50040
2 01-01-02-03-04-05 WGSW-50040                   MIS_zebra
```

2.17 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 WGSW-50040          LAB_SWITCH_1 CM 01-02-03-04-05-01 -root-           -root-           -
      2 WGSW-50040          LAB_SWITCH_2 M    01-02-03-04-05-02 eth 1/1          eth 1/2          N
      3 WGSW-50040          LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/1          eth 1/3          Y
      4 WGSW-50040          LAB_SWITCH_4 CA 01-02-03-04-05-04 eth 1/1          eth 1/4          Y
..............................................................................
2     2 WGSW-50040          LAB_SWITCH_2 M    01-02-03-04-05-02 eth 1/1          eth 1/2          -
      5 WGSW-50040          LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1          eth 1/2          Y
      6 WGSW-50040          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 WGSW-50040          LAB_SWITCH_2 M    01-02-03-04-05-02 eth 1/1          eth 1/2          -
      5 WGSW-50040          LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1          eth 1/2          Y
      6 WGSW-50040          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: WGSW-50040
```

```
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: WGSW-50040
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
```

2.18 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
```

2.19 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 3 Commands for Network Port Configuration

3.1 Commands for Ethernet Port Configuration

3.1.1 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.

Note

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
```

3.1.2 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**
Fiber 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.

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
```

3.1.3 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
```

3.1.4 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
```

3.1.5 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)#
```

3.1.6 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
```

3.1.7 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
```

3.1.8 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
```

3.1.9 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
```

3.1.10 port-scan-mode

Command:

port-scan-mode {interrupt | poll}

no port-scan-mode

Function:

Configure the scan mode of the port as “interrupt” or “poll”, the no command restores the default scan mode.

Parameters:

interrupt: the interrupt mode;

poll: the poll mode.

Command mode:

Global Mode.

Default:

Poll mode.

Usage Guide:

There are two modes that can respond up/down event of the port. The interrupt mode means that interrupt hardware to announce the up/down change, the poll mode means that software poll can obtain the port event, the first mode is rapid. If using poll mode, the convergence time of MRPP is several hundred milliseconds, if using interrupt mode, the convergence time is less than 50 milliseconds.

Note

The scan mode of the port usually configured as poll mode, the interrupt mode is only used to the environment of the good performance, but the security of the poll mode is better.

Example:

Configure the scan mode of the port as interrupt mode.

```
Switch(config)#port-scan-mode interrupt
```

3.1.11 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
```

3.1.12 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
```

3.1.13 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 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
```

3.1.14 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
```

3.1.15 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 4 Commands for Port Loopback Detection Function

4.1 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
```

4.2 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
```

4.3 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
```

4.4 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
```

4.5 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
```

4.6 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 5 Commands for Port Channel

5.1 debug lacp

Command:

debug lacp

no debug lacp

Function:

Enables the LACP debug function: "**no debug lacp"** command disables this debug function.

Command mode:

Admin Mode.

Default:

LACP debug information is disabled by default.

Usage Guide:

Use this command to enable LACP debugging so that LACP packet processing information can be displayed.

Example:

Enabling LACP debug.

```
Switch# debug lacp
```

5.2 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)#
```

5.3 port-group

Command:

Command: port-group *<port-group-number>* [load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip}]

no port-group *<port-group-number>* [load-balance]

Function:

Creates a port group and sets the load balance method for that group. If no method is specified, the default load balance method is used. The no command deletes that group or restores the default load balance setting. Enter load-balance for restoring default load balance, otherwise, the group will be deleted.

Parameters:

<port-group-number> is the group number of a port channel from 1 to 128, if the group number is already exist, an error message will be given.

dst-mac performs load balancing according to destination MAC;

src-mac performs load balance according to source MAC;

dst-src-mac performs load balancing according to source and destination MAC;

dst-ip performs load balancing according to destination IP;

src-ip performs load balancing according to source IP;

dst-src-ip performs load balancing according to destination and source IP. If a port group has formed a port-channel, the load balance setting cannot be modified, please set the load balance mode before port-channel.

Default:

Switch ports do not belong to a port channel by default; LACP not enabled by default.

Command mode:

Global Mode

Example:

Creating a port group and setting the default load balance method.

```
Switch(config)# port-group 1
```

Delete a port group.

```
Switch(config)#no port-group 1
```

5.4 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 32;

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
```

5.5 show port-group

Command:

show port-group [<*port-group-number*>] {brief | detail | load-balance | port | port-channel}

Parameters:

<port-group-number> is the group number of port channel to be displayed, from 1 to 32;

brief displays summary information;

detail displays detailed information;

load-balance displays load balance information;

port displays member port information;

port-channel displays port aggregation information.

Command mode:

Admin and Configuration Mode.

Usage Guide:

If port-group-number is not specified, then information for all port groups will be displayed.

Example:

1. Display the summary information of port-group 1.

```
Switch#sho 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,
    the first is selected ports number, the second is standby ports number, and
    the third is unselected ports number.

ID   Mode    Partner ID             Ports      Load-balance
--------------------------------------------------------------
1    active   0x8000,0012-cf4d-e1a1    8,1,1      dst-src-mac
10   passive  0x8000,0012-cf4d-e1b2    8,2,0      dst-src-ip
20   on                              8,0,0      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: active,    Load-balance: dst-src-mac
Port-group detail information:
System ID: 0x8000,0003-0f0c-166d
```

```
Local:
Port              Status       Priority   Oper-Key Flag
---------------------------------------------------------
Ethernet1/1       Selected     32768      1        {ACDEF}
Ethernet1/2       Selected     32768      1        {ACDEF}
Ethernet1/3       Selected     32768      1        {ACDEF}
Ethernet1/4       Selected     32768      1        {ACDEF}
Ethernet1/5       Selected     32768      1        {ACDEF}
Ethernet1/6       Selected     32768      1        {ACDEF}
Ethernet1/7       Selected     32768      1        {ACDEF}
Ethernet1/8       Selected     32768      1        {ACDEF}
Ethernet1/20      Unselected   32768      1        {ACG}
Ethernet1/23      Standby      32768      1        {AC}

Remote:
Actor            Partner   Priority   Oper-Key SystemID                  Flag
---------------------------------------------------------------------------
Ethernet1/1      1         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/2      2         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/3      3         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/4      4         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/5      5         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/6      6         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/7      7         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/8      8         32768      1        0x8000,0003-0f01-0204     {CDEF}
Ethernet1/23     23        32768      1        0x8000,0003-0f01-0204     {C}
Switch#
```

3. Display load balance information for port-group 1.

```
Switch# show port-group 1 load-balance
The loadbalance of the group 1 based on src MAC address.
```

4. Display member port information for port-group 1.

```
Switch# show port-group 1 port
Sorted by the ports in the group 1 :
-------------------------------------------
the portnum is 1
port Ethernet1/1 related information:
```

```
Actor part
                        Administrative        Operational
port number                   1
port priority              0x8000
aggregator id                 0
port key                    0x0100              0x0101
port state
LACP activety                 .                   1
LACP timeout                  .                   .
Aggregation                   1                   1
Synchronization               .                   .
Collecting                    .                   .
Distributing                  .                   .
Defaulted                     1                   1
Expired                       .                   .

Partner part
                       Administrative       Operational
system                  000000-000000       000000-000000
system priority            0x8000              0x8000
key                       0x0001              0x0001
port number                   1                   1
port priority              0x8000              0x8000
port state
LACP activety                 .                   .
LACP timeout                  1                   1
Aggregation                   1                   1
Synchronization               .                   .
Collecting                    .                   .
Distributing                  .                   .
Defaulted                     1                   1
Expired                       .                   .

Selected                                      Unselected
```

Displayed information	Explanation
portnumber	Port number
port priority	Port Priority

system	System ID
system priority	System Priority
LACP activety	Whether port is added to the group in active mode, 1 for yes.
LACP timeout	Port timeout mode, 1 for short timeout.
Aggregation	Whether aggregation is possible for the port, 0 for independent port that does not allow aggregation.
Synchronization	Whether port is synchronized with the partner end.
Collecting	Whether status of port bound status machine is collecting or not.
Distributing	Whether status of port bound status machine is distributing or not.
Defaulted	Whether the local port is using default partner end parameter.
Expired	Whether status of port receiving status machine is expire or not.
Selected	Whether the port is selected or not..

5. Display port-channel information for port-group1.

```
Switch# show port-group 1 port-channel
Port channels in the group 1:
----------------------------------------------------------
Port-Channel: port-channel1
Number of port : 2          Standby port : NULL

Port in the port-channel :

Index              Port                Mode
-----------------------------------------------------
1                  Ethernet1/1      active
2                  Ethernet1/2      active
```

Displayed information	Explanation
Port channels in the group	If port-channel does not exist, the above information will not be displayed.
Number of port	Port number in the port-channel.
Standby port	Port that is in “standby” status, which means the port is qualified to join the channel but cannot join the channel due to the maximum port limit, thus the port status is standby instead of selected.

Chapter 6 Commands for Jumbo

6.1 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.

Parameters:

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.

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 7 VLAN Configuration

7.1 Commands for VLAN Configuration

7.1.1 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
```

7.1.2 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)#
```

7.1.3 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)#
```

7.1.4 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
```

7.1.5 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
```

7.1.6 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
```

7.1.7 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
```

7.1.8 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
```

7.1.9 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
```

7.1.10 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
```

7.1.11 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
```

7.1.12 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
Interface Ethernet1/3:
dot1q-tunnel is enable
```

7.1.13 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.

Example:

Display global GARP information.

```
Switch #show garp
```

7.1.14 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.

Example:

Display global GVRP information.

```
Switch#show gvrp configuration
---------------- Gvrp Information ------------------
Gvrp status : enable
Gvrp Timers(milliseconds)
LeaveAll       :   10000
```

7.1.15 show vlan

Command:

show vlan [brief | summary] [id <*vlan-id*>] [name <*vlan-name*>] [internal usage [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.

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
```

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

7.1.16 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
```

7.1.17 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
```

7.1.18 switchport mode

Command:

switchport mode {trunk | access}

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.

Example:

Set port 5 to trunk mode and port 8 to access 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
```

7.1.19 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
```

7.1.20 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
```

7.1.21 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)#
```

7.1.22 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
```

7.2 Commands for Dynamic VLAN Configuration

7.2.1 dynamic-vlan mac-vlan prefer

Command:

dynamic-vlan mac-vlan prefer

Function:

Set the MAC-based VLAN preferred.

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
```

7.2.2 dynamic-vlan subnet-vlan prefer

Command:

dynamic-vlan subnet-vlan prefer

Function:

Set the IP-subnet-based VLAN preferred.

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
```

7.2.3 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
```

7.2.4 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
```

7.2.5 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
```

7.2.6 show dynamic-vlan prefer

Command:

show dynamic-vlan prefer

Function:

Display the preference of the dynamic VLAN.

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
```

7.2.7 show mac-vlan

Command:

show mac-vlan

Function:

Display the configuration of MAC-based VLAN on the switch.

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
```

7.2.8 show mac-vlan interface

Command:

show mac-vlan interface

Function:

Display the ports at MAC-based VLAN.

Command Mode:

Admin Mode and other configuration Mode.

Usage Guide:

Display the ports at MAC-based VLAN.

Example:

Display the ports of enabling MAC-based VLAN currently.

```
Switch#show mac-vlan interface
Ethernet1/1          Ethernet1/2
Ethernet1/3          Ethernet1/4
Ethernet1/5          Ethernet1/6
```

7.2.9 show protocol-vlan

Command:

show portocol-vlan

Function:

Display the configuration of Protocol-based VLAN on the switch.

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
```

7.2.10 show subnet-vlan

Command:

show subnet-vlan

Function:

Display the configuration of the IP-subnet-based VLAN on the switch.

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
```

7.2.11 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 at IP-subnet-based VLAN.

Example:

Display the port of enabling IP-subnet-based VLAN currently.

```
SwitchA#show subnet-vlan interface
Ethernet1/1          Ethernet1/2
Ethernet1/3          Ethernet1/4
```

7.2.12 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
```

7.2.13 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.

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
```

7.2.14 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.

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
```

7.3 Commands for Voice VLAN Configuration

7.3.1 show voice-vlan

Command:

show voice-vlan

Function:

Display the configuration status of the Voice VLAN on the switch.

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
```

7.3.2 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.

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
```

7.3.3 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
```

7.3.4 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 8 Commands for MAC Address Table Configuration

8.1 Commands for MAC Address Table Configuration

8.1.1 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
```

8.1.2 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
```

8.1.3 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
```

8.2 Commands for Mac Address Binding configuration

8.2.1 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
```

8.2.2 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.

8.2.3 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.

8.2.4 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.

8.2.5 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
```

8.2.6 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
```

8.2.7 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
```

8.2.8 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
```

8.2.9 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
```

8.2.10 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
```

8.2.11 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 9 Commands for MSTP

9.1 Commands for MSTP

9.1.1 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)#
```

9.1.2 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)#
```

9.1.3 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
```

9.1.4 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
```

9.1.5 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
```

9.1.6 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
```

9.1.7 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
```

9.1.8 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
```

9.1.9 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
```

9.1.10 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
```

9.1.11 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
```

9.1.12 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
```

9.1.13 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
```

9.1.14 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)#
```

9.1.15 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 64.

<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
```

9.1.16 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 64;

<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
```

9.1.17 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 64;

<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
```

9.1.18 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)#
```

9.1.19 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)#
```

9.1.20 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
```

9.1.21 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)#
```

9.1.22 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.

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)#
```

9.1.23 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)#
```

9.1.24 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)#
```

9.2 Commands for Monitor and Debug

9.2.1 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 64;

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

9.2.2 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
---------------------------------
```

9.2.3 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)#
```

9.2.4 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 10 Commands for QoS

10.1 accounting

Command:

accounting

no accounting

Function:

Set statistic function for the classified traffic.

Default:

Policy map configuration mode

Command mode:

Do not set statistic function.

Usage Guide:

After enable this function, add statistic function to the traffic of the policy class map. In 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. In the print information, in-profile means green and out-profile means red and yellow.

Example:

Count the packets which satisfy c1 rule.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#accounting
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

10.2 class

Command:

class <*class-map-name*> [insert-before <*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.

insert-before ***<class-map-name>*** insert a new configured class to the front of a existent class to improve the priority of the new 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:

After add a policy class map c1 to the policy map, add a policy class map c2 and insert it to the front of c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#class c2 insert-before c1
Switch(Config-PolicyMap-p1-Class-c2)#exit
```

10.3 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

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
```

10.4 class mls qos statistics

Command:

clear mls qos statistics [interface <*interface-name*> | vlan <*vlan-id*>]

Function:

Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.

Parameters:

***<vlan-id>*:** VLAN ID.

***<interface-name>*:** The interface name.

Default:

Do not set action.

Command mode:

Admin Mode

Usage Guide:

Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.

Example:

Clear the Policy Map statistic of VLAN 100.

```
Switch#Clear mls qos statistics vlan 100
```

10.5 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 <*cos-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, the ranging is 0~63;

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, the ranging is 1~4094;

<*cost-list*> match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the ranging is 0~7.

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 the match ACL, permit rule as the match option, apply Policy Map action. Deny rule as the excluding option, do not apply Policy Map action. If configure another match rule after one was configured, the operation fails, but configure the same match rule will cover the previous.

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
```

10.6 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
```

10.7 mls qos map

Command:

Command: mls qos map (cos-dp <dp1…dp8> | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp>)

no mls qos map (cos-dp | dscp-dscp | dscp-intp | dscp-dp)

mls qos map intp-dscp <dscp1..dscp8>

no mls qos map intp-dscp

Function:

Set the priority mapping of QoS, the no command restores the default mapping.

Parameters:

cos-dp <dp1…dp8> defines the mapping from CoS to dp (drop precedence) value,

<dp1..dp8> are 8 dp value corresponding to the 0 to 7 CoS value, each dp value is delimited with space, ranging from 0 to 2;

dscp-dscp defines the mapping from ingress DSCP to egress DSCP,

<in-dscp list> stand for incoming DSCP values, up to 8 values are supported, each DSCP value is delimited with space, ranging from 0 to 63, *<out-dscp>* is the output DSCP value, ranging from 0 to 63;

dscp-intp defines the mapping from DSCP to intp;

dscp-dp defines the mapping from DSCP to dp;

intp-dscp defines the mapping from intp to DSCP,

<dscp1..dscp8> are 8 DSCP value corresponding to the 0 to 7 intp value, each CoS value is delimited with space, ranging from 0 to 63.

Default:

Default mapping values are:

Default CoS-TO-DP Map

CoS Value	0	1	2	3	4	5	6	7
DP Value	0	0	0	0	0	0	0	0

Default DSCP-TO-DSCP Map

In-DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Out-DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-TO-INTP Map

In-DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
INTP Value	0	1	2	3	4	5	6	7

Default DSCP-TO-DP Map

In-DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
DP Value	0	0	0	0	0	0	0	0

Command mode:

Global Mode

Usage Guide:

INTP means the chip internal priority setting, DP means the drop precedence. Because of the internal DSCP value have 64 and the chip internal priority only 8, the dscp-intp mapping need 8 continuum dscp-inside mapping to the same INTP or DP.

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
```

10.8 mls qos queue algorithm

Command:

mls qos queue algorithm {sp | wrr | wdrr}

no mls qos queue algorithm

Function:

After configure this command, the queue management algorithm is set.

Parameters:

sp: The strict priority, the queue number of bigger, then the priority is higher.

wrr: Select wrr algorithm

wdrr: Select wdrr algorithm

Default:

The default queue algorithm is wrr.

Command mode:

Port Mode

Usage Guide:

After configure this command, the queue management algorithm is set.

Example:

Setting the queue management algorithm as wrr.

```
Switch(interface-ethernet1/1/1)#mls qos queue algorithm wrr
```

10.9 mls qos queue wrr weight

Command:

mls qos queue wrr weight <weight0..weight7>

no mls qos queue wrr weight

Function:

After configure this command, the queue weight is set.

Parameters:

<weight0..weight7> defines the queue weight, for WRR algorithm, this configuration is valid, for SP algorithm, this configuration is invalid, when the weight is 0, this queue adopts SP algorithm to manage, and WRR algorithm turns into SP+WRR algorithm. The absolute value of WRR is meaningless. WRR allocates bandwidth by using 8 weight values. The different chips support the different weight range, if the setting exceeds the chip range will prompt the right range, when the chip supports 4 queues, it's parameter turns into <weight1..weight4>.

Default:

The queue weight is 1 2 3 4 5 6 7 8.

Command mode:

Port Mode

Usage Guide:

If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWRR. When removing the queue, the system will manage SP queue at first, then manage WRR queue, SP queue executes the strict priority management mode, WRR queue executes the weight rotation management mode.

Example:

Configure the queue weight as 1 2 3 4 5 6 7 8.

```
Switch(interface-ethernet1/1)#mls qos queue weight 1 2 3 4 5 6 7 8
```

10.10 mls qos queue wdrr weight

Command:

mls qos queue wdrr weight <weight0..weight7>

no mls qos queue wdrr weight

Function:

After configure this command, the queue weight is set.

Parameters:

<weight0..weight7> defines the queue weight, in Kbytes. For WDRR algorithm, this configuration is valid, but for SP algorithm, it is invalid. When the weight is 0, this queue adopts SP algorithm to manage, and WDRR algorithm turns into SP+WDRR algorithm. WRR, in byte, allocates bandwidth by using 8 weight values. The different chips support the different weight range, if the setting exceeds the chip range will prompt the right range, when the chip supports 4 queues, it's parameter turns into <weight1..weight4>.

Default:

The queue weight is 10 20 40 80 160 320 640 1280.

Command mode:

Port Mode

Usage Guide:

If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWDRR. When removing the queue, the system will manage SP queue at first, then manage WDRR queue, SP queue executes the strict priority management mode, WDRR queue executes the weight rotation management mode.

Example:

Configure the queue bandwidth as 10kbytes, 10kbytes, 20kbytes, 20kbytes, 30kbytes, 30kbytes, 40kbytes, 40kbytes.

```
Switch(interface-ethernet1/1)#mls qos queue weight 10 10 20 20 40 40 80 80
```

10.11 mls qos queue bandwidth

Command:

mls qos queue <*queue-id*> bandwidth <*minimum-bandwidth*> <*maximum-bandwidth*>

no mls qos queue <*queue-id*> bandwidth

Function:

After configure this command, the queue bandwidth guarantee is set.

Parameters:

<*queue-id*> is the queue ID to configure the bandwidth guarantee, the different chip supports the different queue count, the range is different too, and the ranging from 1 to 8.

<*minimum-bandwidth* > is the minimum-bandwidth, ranging from 0 to 128000, when input 0, it means the min-bandwidth function is not take effect.

<*maximum-bandwidth* > is the maximum-bandwidth, ranging from 0 to 128000, when input 0, it means the max-bandwidth function is not take effect. The minimum-bandwidth must not bigger than maximum-bandwidth.

Default:

The queue bandwidth have no guarantee.

Command mode:

Port Mode

Usage Guide:

The minimum-bandwidth guarantee and maximum-bandwidth limit can be configured at the different or same queue. The queue bandwidth pledge for egress is relative to management 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 minimum-bandwidth will be satisfied at first, then the excess bandwidth is managed according to SP.

Example:

Configure the minimum-bandwidth is 64kbps and the maximum-bandwidth is 128kbps for ethernet1/2 queue1.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# mls qos queue 1 bandwidth 64 128
```

10.12 mls qos trust

Command:

mls qos trust {cos | dscp}

no mls qos trust {cos | dscp}

Function:

Configures port trust; the no command disables the current trust status of the port.

Parameters:

cos configures the port to trust CoS value; **dscp** configures the port to trust DSCP value.

Default:

Trust CoS value.

Command mode:

Port Configuration Mode.

Usage Guide:

trust **cos mode:** can set the intp value based cos-to-intp mapping, set the message dp value based cos-to-dp mapping.

trust dscp mode: can set the intp field based dscp-to-intp mapping, set the dp value based dscp-to-dp mapping, set DSCP value based dscp-to-dscp mapping.

trust **cos** and **trust dscp** can set at the same time, **trust dscp** priority is bigger than **trust cos** priority.

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
```

10.13 policy

Command:

Single Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION}| exceed-action

ACTION})

Dual Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }]

ACTION definition:

drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value>

no policy

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, set the corresponding action to the different color packets. The no command will delete the mode configuration.

Parameters:

bits_per_second：The committed information rate – CIR (Committed Information Rate), in Kbps, ranging from 1 to 10000000;

normal_burst_bytes：The committed burst size – CBS (Committed Burst Size), in byte, 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 – PBS (Peak Burst Size), in byte, 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 information rate – PIR (Peak Information Rate), in kbps, ranging from 1 to 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 exists in dual bucket mode;

conform-action：The action to take when the CIR is not exceeded, which means the messages are green, the default as transmit;

exceed-action：The actions to take when the CIR is exceeded but PIR isn’t, which means the messages are yellow, the default as drop;

violate-action：The actions to take when the PIR is exceeded, which means the messages are red, the default as drop.

ACTION include:

Drop/transmit: Drop/transmit the packets

set-dscp-transmit sets DSCP, it is valid to IPv4 and IPv6 packets, only set-dscp-transmit or set-prec-transmit can be selected.

set-prec-transmit sets TOS, only set-prec-transmit or set-dscp-transmit can be selected

set-internal-priority sets the internal priority of the packets

set-Drop-Precedence sets the drop precedence of the packets

set-cos-transmit sets the CoS value of the L2 packets

Default:

No policy action; the default action of conform-action is transmit, while that of exceed-action and violate-action both is drop.

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 PIR or PBS is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single bucket dual color; if only PBS is configured, the mode is single rate dual bucket three color; if PIR and PBS are configured, the mode is dual rate dual bucket three color. “set” and “policy”（policy aggregate） are selected and have the same action in Policy Map, then the action selected by “policy” will cover the action of “set”.

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
```

10.14 policy aggregate

Command:

policy aggregate <*aggregate-policy-name*>

no policy aggregate <*aggregate-policy-name*>

Function:

Police Map reference aggregate policy, applies an aggregate policy to classified traffic; the “**no**

policy aggregate <*aggregate-policy-name*>” command deletes the specified aggregate policy.

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
```

10.15 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
```

10.16 set

Command:

set {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos>}

no set {ip dscp | ip precedence | internal priority | drop precedence | 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.

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.

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
```

10.17 service-policy input

Command:

service-policy input <*policy-map-name*>

no service-policy input <*policy-map-name*>

Function:

Applies a policy map to the specified port; the no command deletes the specified policy map applied to the port.

Parameters:

input <*policy-map-name*> applies the specified policy map to the ingress direction of switch port.

Default:

No policy map is bound to port and VLAN interface by default.

Command mode:

Port Configuration Mode.

Usage Guide:

Only one policy map can be applied to each direction of each port or VLAN interface. It is not recommended to use policy map on VLAN and VLAN's port at the same time. 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
```

10.18 service-policy input vlan

Command:

service-policy input <*policy-map-name*> vlan <*vlan-list*>

no service-policy input <*policy-map-name*> vlan < *vlan-list*>

Function:

Applies a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface.

Parameters:

input <*policy-map-name*> applies the specified policy map to the ingress direction of switch VLAN interface.

Default:

No policy map is bound to VLAN interface by default.

Command mode:

Global Configuration Mode.

Usage Guide:

Only one policy map can be applied to each direction of each port or VLAN interface. It is not recommended to use policy map on VLAN and VLAN’s port at the same time. Egress policy map is not supported yet.

Example:

Bind policy p1 to ingress of VLAN interface v2, v3, v4, v6.

```
Switch(config)# service-policy input p1 vlan 2-4;6
```

10.19 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.

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.

10.20 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.

Command mode:

Admin Mode.

Usage Guide:

Displays all configured policy-map or specified policy-map information.

Example:

```
Switch # show policy -map
Policy Map p1, used by 0 port
  Class Map name: c1
    policy CIR: 1000 CBS: 1000   PIR: 200 PBS: 3000
    conform-action:
     transmit
    exceed-action:
     drop
    violate-action:
     drop
```

Displayed information	Explanation
Policy Map p1	Name of policy map

Class map name:c1	Name of the class map referred to
policy CIR: 1000 CBS: 1000 PIR: 200 PBS: 3000 conform-action: transmit exceed-action: drop violate-action: drop	Policy implemented

10.21 show mls qos interface

Command:

show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>} | [begin | include | exclude <regular-expression>]

Function:

Displays QoS configuration information on a port.

Parameters:

<interface-id> is the port ID;

<vlan-id>: VLAN ID;

policy is the policy setting on the port;

queuing is the queue setting for the port.

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
  Trust：COS DSCP EXP
  Attached Policy Map for Ingress: p1
  Classmap      classified      in-profile      out-profile (in packets)
  c1          20           10           10
  c2          NA           NA           NA
（If there is no Accounting for Class Map, show NA）

Internal-Priority-TO-Queue map:
INTP        0     1     2     3     4     5     6     7
-----------------------------------------------------------------------------
Queue       0     1     2     3     4     5     6     7

Queue Algorithm：WRR
Queue weights：
Queue       0     1     2     3     4     5     6     7
-----------------------------------------------------------------------------------------------------------
weight       1     2     3     4     5     6     7     8

Bandwidth Guarantee Configuration:
Queue       0     1     2     3     4     5     6     7
-----------------------------------------------------------------------------------------------------------
MinBW(K)    128    0      0     0     0      0      0     0
MaxBW(K)   256   0   0     0     0      0      0     0
```

Display Information	Explanation
Ethernet1/2	Port name
default cos:0	Default CoS value of the port
Trust：COS DSCP EXP	The trust state of the port
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap. If there is no Accounting for Class Map, show NA
in-profile	Total in-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
out-profile	Total out-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm：	WRR or PQ queue out method

Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

```
Switch(config)#show mls qos interface ethernet1/2 queuing
Ethernet1/2:
  Internal-Priority-TO-Queue map:
   INTP    0      1      2      3      4      5      6      7
  ------------------------------------------------------------------------------
  Queue    0      1      2      3      4      5      6      7

   Queue Algorithm：WRR
   Queue weights：
   Queue        0      1      2      3      4      5      6      7
   ---------------------------------------------------------------------------------------------------------
   weight        1      2      3      4      5      6      7      8

   Bandwidth Guarantee Configuration:
   Queue        0      1      2      3      4      5      6      7
   ---------------------------------------------------------------------------------------------------------
   MinBW(K)    128     0        0       0       0         0        0       0
  MaxBW(K)   256     0    0       0       0         0        0       0
```

Display Information	Explanation
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm：	WRR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

```
Switch # show mls qos interface policy ethernet 1/2
Ethernet1/2
Attached policy map for Ingress: p1
Accounting：ON
Classmap      classified      in-profile      out-profile (in packets)
        c1              0                    0                    0
```

Display Information	Explanation

Ethernet1/2	Port name
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap.
in-profile	Total in-profile data packets match this ClassMap.
out-profile	Total out-profile data packets match this ClassMap.

```
Switch #show mls qos vlan 100
Vlan 100：
  Attached Policy Map for Ingress: p1
  Classmap     classified     in-profile     out-profile (in packets)
    c1            20              10              10
         c2           NA              NA              NA
```

10.22 show mls qos maps

Command:

show mls qos maps [cos-dp | dscp-dscp | dscp-intp | dscp-dp | intp-dscp] | [begin | include | exclude <regular-expression>]

Function:

Display the configuration of QoS mapping.

Parameters:

cos-dp: The mapping from ingress L2 CoS to drop precedence

dscp-dscp: The mapping from ingress DSCP to DSCP

dscp-intp: The mapping from ingress DSCP to internal priority

dscp-dp: The mapping from ingress DSCP to drop precedence

intp-dscp: The mapping from egress internal priority to DSCP

Command mode:

Admin and Configuration Mode.

Usage Guide:

Display the map configuration information of QoS.

Example:

Display configuration information of the mapping table.

```
Switch # show mls qos maps
```

```
Ingress COS-TO-Drop-Precedence map:
COS        0     1     2     3     4     5     6     7
-----------------------------------------------------------
DP         0     0     0     0     0     0     0     0

Ingress DSCP-TO-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

Ingress DSCP-TO-Internal-Priority map:
d1 : d2   0    1    2    3    4    5    6    7    8    9
0:        0 0    0    0    0    0    0    0    1    1
1:        1    1    1    1    1    1    2    2    2    2
2:        2    2 2    2    3    3    3    3    3    3
3:        3 3    4    4    4    4    4    4    4    4
4:        5 5    5    5    5    5    5    5    6    6
5:        6 6    6    6    6    6    7    7    7    7
6:        7 7    7    7

Ingress DSCP-TO-Drop-Precedence map:
d1 : d2   0    1    2    3    4    5    6    7    8    9
0:        0 0    0    0    0    0    0    0    0    0
1:        0    0    0    0    0    0    0    0    0    0
2:        0    0    0    0    0    0    0    0    0    0
3:        0    0    0    0    0    0    0    0    0    0
4:        0    0    0    0    0    0    0    0    0    0
5:        0    0    0    0    0    0    0    0    0    0
6:        0    0    0    0
Egress Internal-Priority-TO-DSCP map
INTP:      0     1     2     3     4     5     6     7
-----------------------------------------------------------------
DSCP:      0     8     16    24    32    40    48    56
```

10.23 show mls qos vlan

Command:

show mls qos vlan <v-id>

Function:

v-id: the ranging from 1 to 4094.

\Example:

```
Switch#show mls qos vlan 1
```

Chapter 11 Commands for Flow-based Redirection

11.1 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 Port 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
```

11.2 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 12 Commands for Layer 3 Forwarding

12.1 Commands for Layer 3 Interface

12.1.1 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
```

12.1.2 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.

Parameters:

<*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.

Default:

The system default is no IP address configuration.

Command mode:

VLAN interface configuration mode

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
```

12.1.3 ip default-gatway

Command:

ip default-gateway <*ip-address*>

no ip default-gateway <*ip-address*>

Function:

Set the default-gateway address of switch; the no command will delete the default-gateway address.

Parameters:

<*ip-address*> is default-gateway IP address, dotted decimal notation.

Default:

The system default is no IP address configuration.

Command mode:

Global configuration mode

Usage Guide:

The IP address of default-gateway and the IP address of layer 3 interface in the same segment to make sense for default-gateway.

Example:

The IP address of layer 3 interface is 2.2.2.2, network mask is 255.255.255.0, set the IP address of default-gateway is 2.2.2.1.

```
Switch(config)#ip default-gateway 2.2.2.1
```

12.1.4 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.

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 packet
IP PACKET: rcvd, src1.1.1.1, dst1.1.1.2, size 100
```

12.1.5 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
TcpInErrs                 0, TcpInSegs                  3180
TcpMaxConn                0, TcpOutRsts                 3
TcpOutSegs                0, TcpPassiveOpens            8
TcpRetransSegs            0, TcpRtoAlgorithm            0
TcpRtoMax                 0, TcpRtoMin                  0
UDP statics:
UdpInDatagrams            0, UdpInErrors                0
UdpNoPorts                0, UdpOutDatagrams            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.
TcpActiveOpens 0,TcpAttemptFails 0	Active open the connection number, attempt fail number.
TcpCurrEstab 0, TcpEstabResets 0	Current establish the connection number, establish reset number.
TcpInErrs 0, TcpInSegs 3180	Receive error packeages, receive packeage number in segment.
TcpMaxConn 0, TcpOutRsts 3	The max connection number, output reset number.
TcpOutSegs 3, TcpPassiveOpens 8	Output segment packeage number, passive connection number.
TcpRetransSegs 0, TcpRtoAlgorithm 0	Retransfer packeage number, retransfer the time of timer.
TcpRtoMax 0, TcpRtoMin 0	Retransfer the max time is allowed by timer, retransfer the min time is allowed by timer.
UDP statistics:	UDP packet statistics.

UdpInDatagrams 0,UdpInErrors 0 UdpNoPorts 0, UdpOutDatagrams 0	Receive UDP data packets, receive error data packets. No port packeage number, seng packeage number.

12.1.6 show ip route

Command:

show ip route [database]

Function:

Display routing table.

Parameter:

database is database information.

Command mode:

Admin Mode

Usage Guide:

Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.

Example:

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived
Destination Mask Nexthop Interface Pref
C 2.2.2.0 255.255.255.0 0.0.0.0 vlan2 0
C 4.4.4.0 255.255.255.0 0.0.0.0 vlan4 0
S 6.6.6.0 255.255.255.0 9.9.9.9 vlan9 1
```

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.

12.2 Commands for IPv6 configuration

12.2.1 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
```

12.2.2 debug ipv6 packet

Command:

debug ipv6 packet

no debug ipv6 packet

Function:

IPv6 data packets receive/send debug message.

Command Mode:

Admin Mode

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

12.2.3 debug ipv6 icmp

Command:

debug ipv6 icmp

no debug ipv6 icmp

Function:

ICMP data packets receive/send debug message.

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

12.2.4 debug ipv6 nd

Command:

debug ipv6 nd [ns | na | rs | ra | redirect]

no debug ipv6 nd [ns | na | rs | ra | redirect]

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.

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

12.2.5 ipv6 default-gateway

Command:

ipv6 default-gateway <*ipv6-address*>

no ipv6 default-gateway <*ipv6-address*>

Function:

Set the IPv6 default-gateway address of switch; the no command will delete the IPv6 default-gateway address.

Parameter:

<ipv6-address> is default-gateway IPv6 address.

Default:

The system default is no IPv6 address configuration.

Command Mode:

Global configuration mode

Usage Guide:

The IPv6 address of default-gateway and the IPv6 address of layer 3 interface in the same segment to make sense for default-gateway.

Example:

The IPv6 address of layer 3 interface is 2002:10::2/64, set the IPv6 address of default-gateway is 2002:10::1.

```
Switch(config)#ipv6 default-gateway 2002:10::1
```

12.2.6 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:

<ipv6-address> is the prefix of IPv6 address,

<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.

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.

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
```

12.2.7 ipv6 redirect

Command:

ipv6 redirect

no ipv6 redirect

Function:

Enable IPv6 router redirect function. The no operation of this command will disable the function.

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
```

12.2.8 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
```

12.2.9 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:

<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.

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
```

12.2.10 ipv6 nd suppress-ra

Command:

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Function:

Prohibit router announcement.

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
```

12.2.11 ipv6 nd ra-lifetime

Command:

ipv6 nd ra-lifetime <*seconds*>

no ipv6 nd ra-lifetime

Function:

Configure the lifetime of router announcement.

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
```

12.2.12 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
```

12.2.13 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:

<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
```

12.2.14 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:

<*ipv6-prefix*> is the address prefix of the specified announcement,

<*prefix-length*> is the length of the address prefix of the specified announcement,

<*valid-lifetime*> is the valid lifetime of the prefix,

<*preferred-lifetime*> is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime.

no-autoconfig says this prefix can not be used to automatically configure IPv6 address on the host in link-local.

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
```

12.2.15 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:

ipv6-address is static neighbor IPv6 address, same to interface prefix 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:

Pv6 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
```

12.2.16 show ipv6 interface

Command:

show ipv6 interface {brief|<*interface-name*>}

Function:

Show interface IPv6 parameters.

Parameter:

brief is the brief summarization of IPv6 status and configuration, and parameter interface-name is Layer 3 interface name.

Command Mode:

Admin and Configuration 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

12.2.17 show ipv6 route

Command:

show ipv6 route [database]

Function:

Display IPv6 routing table.

Parameter:

database is router database.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

show ipv6 route only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router.

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.

12.2.18 show ipv6 neighbors

Command:

show ipv6 neighbors[{vlan|ethernet|tunnel}*interface-number*| ***interface-name*** **| address <*ipv6address*>]**

Function:

Display neighbor table entry information.

Parameter:

{vlan|ethernet|tunnel}*interface-number*|*interface-name* specify the lookup based on interface. ***ipv6-address*** specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

Command Mode:

Admin and Configuration Mode

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)

12.2.19 show ipv6 traffic

Command:

show ipv6 traffic

Function:

Display IPv6 transmission data packets statistics information.

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

12.2.20 show ipv6 enable

Command:

show ipv6 enable

Function:

Display IPv6 transmission function on/off status.

\Command Mode:

Admin and Configuration 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

12.2.21 show ipv6 redirect

Command:

show ipv6 redirect

Function:

Display the state IPv6 redirect switch.

Command Mode:

Admin and Configuration 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
```

12.3 Commands for ARP Configuration

12.3.1 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
```

12.3.2 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
```

12.3.3 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.
```

12.3.4 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.

12.3.5 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 13 Commands for ARP Scanning Prevention

13.1 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.

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
```

13.2 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
```

13.3 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
```

13.4 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
```

13.5 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
```

13.6 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.

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
```

13.7 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
```

13.8 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.

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
```

13.9 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.

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
```

13.10 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.

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
```

13.11 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.

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 14 Command for ARP GUARD

14.1 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 15 Commands for DHCP

15.1 Commands for DHCP Server Configuration

15.1.1 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

15.1.2 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

15.1.3 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

15.1.4 clear ip dhcp server statistics

Command:

clear ip dhcp server statistics

Function:

Deletes the statistics for DHCP server, clears the DHCP server count.

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

15.1.5 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

15.1.6 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.

15.1.7 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
```

15.1.8 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
```

15.1.9 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

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
```

15.1.10 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

15.1.11 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

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

15.1.12 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

15.1.13 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
```

15.1.14 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)#
```

15.1.15 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.

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

15.1.16 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

15.1.17 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

15.1.18 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
```

15.1.19 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
```

15.1.20 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
```

15.1.21 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
```

15.1.22 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
```

15.1.23 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

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
```

15.1.24 service dhcp

Command:

service dhcp

no service dhcp

Function:

Enables DHCP server; the “**no service dhcp**” command disables the DHCP service.

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
```

15.1.25 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.

15.1.26 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.

15.1.27 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

Chapter 16 Commands for DHCP Snooping

16.1 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.

16.2 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.

16.3 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.

16.4 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.

16.5 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.

16.6 ip dhcp snooping

Command:

ip dhcp snooping enable

no ip dhcp snooping enable

Function:

Enable the DHCP Snooping function.

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
```

16.7 ip dhcp snooping binding

Command:

ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function:

Enable the DHCP Snooping binding funciton

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

16.8 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

16.9 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.

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

16.10 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.

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

16.11 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.

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

16.12 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

16.13 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.

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
```

16.14 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
```

16.15 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 of 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
```

16.16 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.

Example:

Set the message transmission rate as 50pps.

```
switch(config)#ip dhcp snooping limit-rate 50
```

16.17 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.

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
```

16.18 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.

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

16.19 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
```

16.20 ip user private packet version two

Command:

ip user private packet version two

no ip user private packet version two

Function:

The switch choose private packet version two to communicate with trustview.

Command Mode:

Global Mode.

Default:

The switch choose private packet version one to communicate with DCBI.

Usage Guide:

If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.

Example:

To configure the switch choose private packet version two to communicate with inter security management background system.

```
switch(config)#ip user private packet version two
```

16.21 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
```

16.22 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.

Command Mode:

Admin and Configuration Mode.

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
```

16.23 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.

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

16.24 show ip dhcp snooping binding all

Command:

show ip dhcp snooping binding all

Function:

Display the current global binding information of DHCP snooping.

Command Mode:

Admin and Configuration Mode.

Usage Guide:

his command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state.

Example:

```
switch#show ip dhcp snooping binding all
ip dhcp snooping static binding count:1169, dynamic binding count:0

MAC                  IP address        Interface       Vlan ID   Flag
-----------------------------------------------------------------------
00-00-00-00-11-11   192.168.40.1      Ethernet1/1      1         S
00-00-00-00-00-10   192.168.40.10     Ethernet1/2      1         D
00-00-00-00-00-11   192.168.40.11     Ethernet1/4      1         D
00-00-00-00-00-12   192.168.40.12     Ethernet1/4      1         D
00-00-00-00-00-13   192.168.40.13     Ethernet1/4      1         SU
00-00-00-00-00-14   192.168.40.14     Ethernet1/4      1         SU
00-00-00-00-00-15   192.168.40.15     Ethernet1/5      1         SL
00-00-00-00-00-16   192.168.40.16     Ethernet1/5      1         SL
-----------------------------------------------------------------------
The flag explanation of the binding state:
S The static binding is configured by shell command
D The dynamic binding type
U The binding is uploaded to the server
R The static binding is configured by the server
O DHCP response with the option82
L The hardware drive is announced by the binding
X Announcing dot1x module is successful
E Announcing dot1x module is failing
```

Chapter 17 Commands for DHCP Snooping option 82

17.1 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.

Default:

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 “00304f023301”. 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.

Example:

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
```

Chapter 18 IPv4 Multicast Protocol

18.1 Commands for DCSCM

18.1.1 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

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)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
Switch(config)#
```

18.1.2 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.

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
```

18.1.3 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.

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)#
```

18.1.4 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.

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
```

18.1.5 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.

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
```

18.1.6 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

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
```

18.1.7 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.

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
```

18.1.8 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**.**

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)#
```

18.1.9 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.

Default:

Disable

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)#
```

18.1.10 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.

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)#
```

18.1.11 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.

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
```

18.1.12 show ip multicast policy

Command:

show ip multicast policy

Function:

Display multicast policy of configuration

Command Mode:

Admin Mode and Global Mode

Usage Guide:

The command displays multicast policy of configuration

Example:

```
Switch#show ip multicast policy
```

18.1.13 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.

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
```

18.1.14 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

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
```

18.2 Commands for IGMP Snooping

18.2.1 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.

Parameter:

<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 access-list 5000 deny ip 10.1.1.0 0.0.0.255
233.0.0.0 0.255.255.255
```

Relative Command:

show ip igmp snooping vlan <1-4094>

18.2.2 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.

Parameter:

<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

18.2.3 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”.

18.2.4 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

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
```

18.2.5 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

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
```

18.2.6 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
```

18.2.7 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

18.2.8 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

Parameter:

<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
```

18.2.9 ip igmp snooping vlan l2-general-querier-version

Command:

ip igmp snooping vlan <vlanid> L2-general-query-version <version>

Function:

Configure igmp snooping.

Parameter:

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
```

18.2.10 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
```

18.2.11 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
```

18.2.12 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
```

18.2.13 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>

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
```

18.2.14 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
```

18.2.15 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
```

18.2.16 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
```

18.2.17 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
```

18.2.18 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
```

18.2.19 show ip igmp snooping

Command:

show ip igmp snooping [vlan <*vlan-id*>]

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*> 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
--------------------------------
```

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

Chapter 19 IPv6 Multicast Protocol

19.1 Commands for MLD Snooping Configuration

19.1.1 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.

Parameter:

<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>

19.1.2 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.

Parameter:

<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

19.1.3 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.

19.1.4 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:

Global Mode

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
```

19.1.5 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
```

19.1.6 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
```

19.1.7 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
```

19.1.8 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
```

19.1.9 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
```

19.1.10 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
```

19.1.11 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
```

19.1.12 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
```

19.1.13 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
```

19.1.14 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
```

19.1.15 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 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
```

19.1.16 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	timeout of the VLAN as l2-general-querier at suppressed status.

time	
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 20 Commands for Multicast VLAN

20.1 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.

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.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan
```

20.2 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.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan association 3, 4
```

Chapter 21 Commands for ACL

21.1 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}|daily| 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 dc_timer
Switch(Config-Time-Range-dc_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-dc_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00
```

21.2 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 timer
Switch(Config-Time-Range-timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26
```

21.3 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
```

21.4 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
```

21.5 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]

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;

<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.

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: P

Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets pass.

```
Switch(config)#access-list 1100 permit any-source-mac any-destination-mac
tagged-eth2
```

21.6 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.

```
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
```

21.7 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
```

21.8 clear access-group statistic interface

Command:

clear access-group statistic [ethernet <*interface-name*>]

Functions:

Empty packet statistics information of assigned interfaces.

Parameters:

<*interface-name*>: Interface name.

Command Mode:

Admin mode

Examples:

Empty packet statistics information of interface.

```
Switch#clear access-group statistic
```

21.9 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
```

21.10 firewall default

Command:

firewall default {permit | deny}

Functions:

Configure default actions of firewall..

Parameters:

permit means to permit data packets to pass;

deny means to deny all data packets to pass.

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
```

21.11 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 16.

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
```

21.12 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 16.

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
```

21.13 ipv6 access-list

Command:

ipv6 access-list <*num-std*> {deny | permit} {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}}

no ipv6 access-list <*num-std*>

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;

<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.

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 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48
```

21.14 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 1-16.

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
```

21.15 {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 1-16.

Command Mode:

Physical Port Mode

Default:

The entry of port is not bound ACL.

Usage Guide: Usage Guide:

One port can bind ingress rules.

There are four kinds of packet head field based on concerned: MAC ACL, IP ACL, MAC-IP ACL and IPv6 ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data packet matches multi types of four 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 MAC ACL and a IPv6 ACL;

2 · When binding four 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
```

21.16 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 16 (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-access-list extended mac_acl
Switch(Config-Mac-Ext-Nacl-mac_acl)#
```

21.17 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 16 (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)#
```

21.18 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
```

21.19 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
```

21.20 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.

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
```

21.21 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> }} [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
```

21.22 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.

```
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
```

21.23 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.

Command Mode:

Admin 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
```

Displayed information	Explanation
access-list 10(used 1 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any source	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.

21.24 show access-group

Command:

show access-group in (interface {Ethernet | Ethernet IFNAME})

Functions:

Display the ACL binding status on the port.

Parameters:

IFNAME*,* Port name.

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 name: Ethernet1/2
IP Ingress access-list used is 1, packet(s) number is 11110.
```

Displayed information	Explanation
interface name: Ethernet 1/1	Tying situation on port Ethernet1/1
IP Ingress access-list used is 100	No. 100 numeric expansion ACL tied to entrance of port Ethernet1/1
packet(s) number is 11110	Number of packets matching this ACL rule

21.25 show firewall

Command:

show firewall

Functions:

Reveal configuration information of packet filtering functions.

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

21.26 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.

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
```

21.27 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.

Command Mode:

Admin 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
```

21.28 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.

Examples:

Create a time-range named admin_timer.

```
Switch(config)#Time-range admin_timer
```

Chapter 22 Commands for 802.1x

22.1 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
```

22.2 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.

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
```

22.3 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
```

22.4 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
```

22.5 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.

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
```

22.6 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
```

22.7 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
```

22.8 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
```

22.9 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: 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
```

22.10 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
```

22.11 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
```

22.12 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
```

22.13 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
```

22.14 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
```

22.15 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)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#dot1x port-control auto
```

22.16 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
```

22.17 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
```

22.18 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
```

22.19 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
```

22.20 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
```

22.21 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
```

22.22 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
```

22.23 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
```

22.24 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.

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
```

22.25 dot1x web authentication ipv6 passthrough

Command:

dot1x web authentication ipv6 passthrough

no dot1x web authentication ipv6 passthrough

Function:

Enable IPv6 passthrough function on a switch port, only applicable when access control mode is webbased; the no operation of this command will disable the function.

Default:

IPv6 passthrough function is disabled.

Command mode:

Port Mode.

Usage Guide:

The function can only be enabled when 802.1x function is enabled both globally and on the port, web authentication function is enabled and redirect URL is set, with webbased being the control access mode. After it is enabled, users can send IPv6 messages without authentication.

Example:

Enable IPv6 passthrough function on port Ethernet1/12.

```
Switch(config)#dot1x enable
Switch(config)#dot1x web authentication enable
Switch(config)#dot1x web redirect http://10.1.1.1/
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
Switch(Config-If-Ethernet1/12)#dot1x port-method webbased
Switch(Config-If-Ethernet1/12)#dot1x web authentication ipv6 passthrough
```

22.26 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/
```

22.27 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.

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.

Example:

Enable the unauthenticated user to visit the redirect function through Web.

```
Switch(Config)# dot1x web redirect enable
```

22.28 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:

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 23 Commands for the Number Limitation Function of Port, MAC in VLAN and IP

23.1 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
```

23.2 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
```

23.3 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
```

23.4 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:

Any 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
----------------------------------------------------------------------------------------------------
```

23.5 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.

Command Mode:

Admin Mode

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 !!
```

23.6 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.

Command Mode:

Admin Mode.

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 !!
```

Chapter 24 Commands for AM Configuration

24.1 am enable

Command:

am enable

no am enable

Function:

Globally enable/disable AM function.

Default:

AM function is disabled by default.

Command Mode:

Global Mode.

Default:

AM function is disabled on all port.

Example:

Enable AM function on the switch.

```
Switch(config)#am enable
```

Disable AM function on the switch.

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

24.2 am port

Command:

am iport

no am port

Function:

Enable/disable AM function on port.

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
```

24.3 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.

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
```

24.4 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.

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
```

24.5 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

Example:

Delete all configured IP address pools.

```
Switch(config)#no am all ip-pool
```

24.6 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 25 Commands for Security Feature

25.1 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.

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
```

25.2 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.

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
```

25.3 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.

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
```

25.4 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.

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
```

25.5 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.

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.

```
Switch(config)# dosattack-check tcp-fragment enable
```

25.6 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
```

25.7 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.

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
```

25.8 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
```

25.9 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 26 Commands for TACACS+

26.1 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
```

26.2 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
```

26.3 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
```

26.4 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
```

26.5 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

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 27 Commands for RADIUS

27.1 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.

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
```

27.2 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
```

27.3 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
```

27.4 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
```

27.5 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
```

27.6 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.

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
```

27.7 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.

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
```

27.8 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.

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
```

27.9 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
```

27.10 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
```

27.11 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
```

27.12 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
```

27.13 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
```

27.14 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
```

27.15 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
```

27.16 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
```

27.17 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:

Table 7-1 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
```

27.18 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:

```
Switch#show aaa authenticated-user
------------------------ authenticated users ------------------------------
 UserName   Retry RadID Port EapID ChapID OnTime      UserIP            MAC
---------------------------------------------------------------------------


         -------------- total: 0 --------------
```

27.19 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 --------------
```

27.20 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
```

27.21 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 28 Commands for MRPP

28.1 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

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
```

28.2 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.

Example:

Clear statistic information of MRPP ring 4000 of switch.

```
Switch#clear mrpp statistics 4000
```

28.3 debug mrpp

Command:

debug mrpp

no debug mrpp

Function:

Open MRPP debug information; “**no description**” command disables MRPP debug information.

Command Mode:

Admin Mode

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
```

28.4 enable

Command:

enable

no enable

Function:

Enable configured MRPP ring, the “**no enable**” command disables this enabled MRPP ring.

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
```

28.5 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
```

28.6 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
```

28.7 mrpp enable

Command:

mrpp enable

no mrpp enable

Function:

Enable MRPP protocol module, the "**no mrpp enable**" command disables MRPP protocol.

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
```

28.8 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.

Example:

```
Switch(config)#mrpp ring 100
```

28.9 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

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
```

28.10 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

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
```

28.11 node-mode

Command:

node-mode {maser | transit}

Function:

Configure the type of the node to primary node or secondary node.

Command Mode:

MRPP ring mode

Default:

Default the node mode is secondary node.

Example:

Configure the switch to primary node. MRPP ring 4000.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master
```

28.12 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.

Example:

Display configuration of MRPP ring 4000 of switch

```
Switch# show mrpp 4000
```

28.13 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.

Example:

Display statistic information of MRPP ring 4000 of switch.

```
Switch# show mrpp statistic 4000
```

Chapter 29 Commands for Mirroring Configuration

29.1 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 means the CPU on the board to be the source of the mirror for debugging. Datagram received by or sent by the 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 tx
Switch(config)#monitor session 1 source interface ethernet 1/5 tx
```

29.2 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
```

29.3 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.

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
```

29.4 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 30 Commands for sFlow

30.1 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
```

30.2 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
```

30.3 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
```

30.4 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
```

30.5 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
```

30.6 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
```

30.7 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
```

30.8 show sflow

Command:

show sflow

Function:

Display the sFlow configuration state.

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 31 Commands for SNTP

31.1 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
```

31.2 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
```

31.3 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
```

31.4 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
```

31.5 show sntp

Command:

show sntp

Function:

Displays current SNTP client configuration and server status.

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 32 Commands for Show

32.1 clear logging

Command:

clear logging sdram

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

32.2 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:

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
```

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
```

32.3 logging loghost sequence-number

Command:

logging loghost sequence-number

no logging loghost sequence-number

Function:

Add the loghost sequence-number for the log, the no command does not include the loghost sequence-number.

Command Mode:

Port Mode

Default:

Do not include the sequence-number.

Usage Guide:

Use logging command to configure the loghost before this command is set.

Example:

Open the loghost sequence-number.

```
Switch(config)# logging loghost sequence-number
```

32.4 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:

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.

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.

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.

32.5 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.

32.6 show debugging

Command:

show debugging {l4 | l4drv | nsm | other | spanning-tree}

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 nsm
NSM debugging status
```

Relative command:

Debug

32.7 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 ----
```

32.8 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
```

32.9 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:

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
```

Display all the information which level is warning in the log buffer zone channel.

```
Switch#show logging buffered level warning
```

32.10 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    *................*
```

32.11 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
```

32.12 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.

32.13 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.

32.14 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.

32.15 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
```

32.16 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
```

32.17 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.

32.18 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
```

32.19 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.

32.20 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 33 Commands for Reload Switch after Specified Time

33.1 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

33.2 reload cancel

Command:

reload cancel

Function:

Cancel the specified time period to reload the switch.

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

33.3 show reload

Command:

show reload

Function:

Display the user’s configuration of command “reload after”.

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 34 Commands for Debugging and Diagnosis for Packets Received and Sent by CPU

34.1 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
```

34.2 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
```

34.3 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
```

34.4 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.

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
```

34.5 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 protocol type of the packets, if do not input parameters, show all statistic packets.

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：

Show the statistics of the CPU receiving arp packets.

```
Switch#show cpu-rx protocol arp
Type                     Rate-limit     TotPkts          CurState
arp                     500               3                    allowed
```

34.6 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
```

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product: 50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
*Model Number: WGSW-50040

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 11F, No 96, Min Chuan Road,
Hsin Tien, Taipei, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(1998 + A1:2000 + A2:2003, Class A)
EN 61000-3-2	(2000 + A2:2005 Class D)
EN 61000-3-3	(1955 + A1:2001 + A2:2005)
EN 55024	(1998 + A1:2001 + A2:2003)
IEC 61000-4-2	(1995 + A1:1998 + A2:2000)
IEC 61000-4-3	(2002 + A1:2002)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(1995 + A1:2000)
IEC 61000-4-6	(1996 + A1:2000)
IEC 61000-4-8	(1993 + A1:2000)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** □ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Kent Kang

Taiwan
Place

1th Sep, 2010
Date

Legal Signature